IntraCore 8000
Ethernet Switch

User's Manual

August 2000
Part Number 06-00566-00

Copyright Notice

Trademarks

Asanté Technologies and IntraCore are trademarks of Asanté Technologies, Inc. Ethernet is a registered trademark of the Xerox Corporation. All brand names and products are trademarks or registered trademarks of their respective holders.

FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Operation of this equipment in a residential area is likely to cause interference, in which case, the user, at his or her own risk and expense, will be required to correct the interference.

LIMITED FIVE YEAR WARRANTY

Subject to the limitations and exclusions below, Asanté warrants to the original end user purchaser that the covered products will be free from defects in title, materials and manufacturing workmanship for a period of five years from the date of purchase. This warranty excludes fans, power supplies, non-integrated software and accessories. Asanté warrants that the fans and power supplies will be free from defects in title, materials and manufacturing workmanship for one year from date of purchase. Asanté warrants that non-integrated software included with its products will be free from defects in title, materials, and workmanship for a period of 90 days from date of purchase, and the Company will support such software for the purpose for which it was intended for a period of 90 days from the date of purchase. This warranty expressly excludes problems arising due to compatibility with other vendors products, or future compatibility due to third party software or driver updates.

To take advantage of this warranty, you must contact Asanté for a return materials authorization (RMA) number. The RMA number must be clearly written on the outside of the returned package. Product must be sent to Asanté postage paid. In the event of a defect, Asanté will repair or replace defective product or components with new, refurbished or equivalent product or components as deemed appropriate by Asanté. The foregoing is your sole remedy, and Asanté's only obligation, with respect to any defect or non-conformity. Asanté makes no warranty with respect to accessories (including but not limited to cables, brackets and fasteners) included with the covered product, nor to any discontinued product, i.e., product purchased more than thirty days after Asanté has removed such product from its price list or discontinued shipments of such product.

This warranty is exclusive and is limited to the original end user purchaser only. This warranty shall not apply to secondhand products or to products that have been subjected to abuse, misuse, abnormal electrical or environmental conditions, or any condition other than what can be considered normal use.

ASANTÉ MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, REGARDING THE ASANTÉ PRODUCTS, EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, ALL WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. ASANTÉ'S LIABILITY ARISING FROM OR RELATING TO THE PURCHASE, USE OR INABILITY TO USE THE PRODUCTS IS LIMITED TO A REFUND OF THE PURCHASE PRICE PAID. IN NO EVENT WILL ASANTÉ BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES FOR THE BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, INCLUDING ECONOMIC LOSS, DAMAGE TO PROPERTY AND, TO THE EXTENT PERMITTED BY LAW, DAMAGES FOR PERSONAL INJURY, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE). THESE LIMITATIONS SHALL APPLY EVEN IF ASANTE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF THIS WARRANTY IS FOUND TO FAIL OF ITS ESSENTIAL PURPOSE.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or limitations on how long an implied warranty lasts, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from jurisdiction to jurisdiction.

Table of Contents

1
Introduction

This chapter introduces the IntraCore architecture, then gives a description of the chassis and the various modules that can be installed in the IntraCore 8000. There are also tables of the key features, default settings, and specifications of the IntraCore 8000, and explanations of the different LED indicators used by the various modules.

IntraCore Architecture Overview

Asanté has developed the IntraCore™ Architecture to meet the needs of multi-service networks that support all applications and data types. The architecture is standards-based and provides

- ❑ multi-vendor inter-operability
- ❑ a migration path from current systems
- ❑ investment protection

With the IntraCore Architecture, Asanté has found innovative ways of embracing industry standards and technology advances to create products capable of meeting real world requirements for converged, multi-service networks.

The overall design incorporates a family of tightly integrated ASICs, designed as system building blocks. These building blocks enable the rapid development of advanced networking systems that are timed to meet market requirements. The architecture ensures consistent high performance as systems scale their capacity and feature capability. This approach extends the useful life of the system and protects customer investments.

The Core Switching Engine

The Core Switching Engine is the centerpiece for all IntraCore products. Based on advanced silicon ASICs, the Core Switching Engine is a high performance, non-blocking, multi-gigabit switching fabric with scalable bandwidth capacity. The Core Switching Engine is data format independent and can support either frame or cell based interfaces. This capability is becoming increasingly important as enterprise (primarily frame-based) and service provider (primarily cell-based) networks move closer together.

Infrastructure Connectivity

The second key element of the architecture is Infrastructure Connectivity. IntraCore specifies standards based, high performance, cost effective technologies for connectivity among devices in the network.

In the LAN –

At the network edge, Layer 2 switched 10/100/1000 Ethernet meets the requirements for high-speed connectivity of desktop computers and scalable, cost effective data transmission for trunks to the network core.

In the network core, Layer 2/3+-switched 10/100/1000 Ethernet meets the requirements for high speed, scalable, cost effective data transmission and support for all multi-service data types. High performance servers can be centrally located for added physical security.

Throughout the LAN, advanced queuing techniques combined with multiple priority levels and support for industry standard 802.1Q and 802.1p enable Quality of Service within the network.

In the MAN/WAN –

Long haul Gigabit Ethernet, ATM, and Packet over SONET meet the requirements for all of the following:

- ❑ scalable, cost effective data transmission
- ❑ support for all multi-service data types
- ❑ service provider inter operability

Network Management, Security, Performance, and Control

IntraCore includes a rich suite of features required for the effective management, security, performance, and control of the network. The following table illustrates the features and standards supported by the IntraCore architecture.

Feature	Manage-ment	Security	Perfor-mance	Control
Web Browser Management	Supported			
SNMP, RMON	Supported		Supported	Supported
Standard MIsS	Supported		Supported	Supported
802.1P Priority			Supported	Supported
802.1Q VLAN Tagging	Supported		Supported	Supported
802.1D – Spanning Tree		Supported	Supported	Supported
IGMP V1, V2 Snooping			Supported	Supported
RSVP Snooping			Supported	Supported
GARP Multicast Registration			Supported	Supported
Duplicate IP addr. detection	Supported	Supported		
Station movement notification	Supported	Supported		
IP to MAC address binding	Supported	Supported		
Controlled management access		Supported		
GVRP (Group VLAN Regis-tration Protocol)	Supported		Supported	Supported
Advanced Port Configuration: Broadcast & Multicast rate limit & port priority	Supported		Supported	Supported

Table 1-1 Summary of IntraCore's supported features

The IntraCore Product Family

The Asanté IntraCore architecture is the basis for a family of switching system products in fixed, stackable and chassis form factors that allow customers to integrate telephony, video and data applications. Initially, two systems are offered that provide high performance, high port-count, Layer 2 switching. Additional configurations will be introduced to offer advanced Layer 3 and above routing, traffic classification, advanced QoS, higher bandwidth and port capacity. All systems will be consistent in their

operation and management allowing customers to seamlessly deploy any model in their network.

Edge Switches

Edge Switches provide the first point of connectivity to the network. Connecting to an Enterprise Switch in the network core, Edge Switches provide aggregation of traffic from desktop computers over high capacity trunks. The initial product introduced in the Edge Switch category is the IntraCore 8000.

The IntraCore 8000 is a stackable, high performance solution for enterprise edge applications. Each stack supports up to 192 10/100Mbps switched Ethernet connections for cost-effective high-density connectivity in wiring closets. The system can operate as a stand-alone network or be used in combination with IntraCore 8000 in the backbone.

Enterprise Switches

In the network core, Enterprise Switches are deployed to aggregate traffic from wiring closets and provide high-speed connectivity to network servers. Typically these switches are modular in form factor, and can be easily upgraded or reconfigured. This flexibility provides for customized configurations to meet a wide variety of requirements. The initial product introduced in this category is the IntraCore 9000.

The IntraCore 8000

The IntraCore 8000 is a stackable, high performance solution for enterprise edge applications. Each stack supports up to 192 10/100Mbps switched Ethernet connections for cost-effective high-density connectivity in wiring closets. The system can operate as a stand-alone network or be used in combination with an IntraCore 8000 in the backbone.

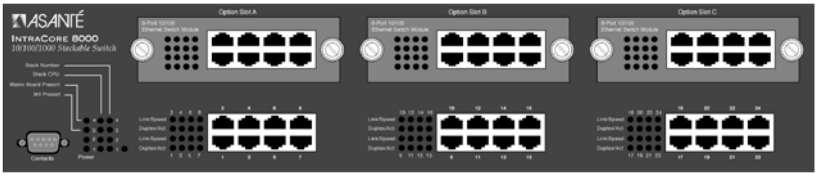


Figure 1-1 IntraCore 8000 Front Panel

Expansion Modules

The following modules can be used to extend the capabilities of the IntraCore 8000.

8-port 10/100 Switch Module

This module provides 8 ports supporting switched 100BaseTX or 10BaseT per port. Each module occupies a single slot and has either 24 RJ-45 connectors or 2 RJ-21 connectors.

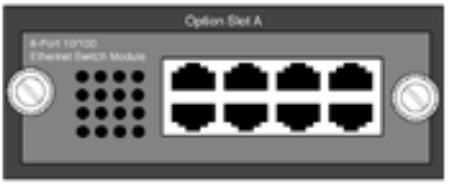


Figure 1-2 8-port 10/100 Switch Module

Gigabit Ethernet Switch Module

This module provides a slot for a switched Gigabit Ethernet port. Each module occupies a single slot and has a GBIC port that accepts Asanté or third party GBIC interfaces. The following subsections describe the possible GBIC interfaces.

Figure 1-3 Gigabit Ethernet Switch Module

1000Base SX GBIC

This module provides a GBIC interface with SC-type fiber connectors. The interface supports 62.5 and 50 micron multimode fiber media. The 62.5 micron multimode fiber can be up to 275 meters long, and the 50 micron multimode fiber can be up to 550 meters long.

1000BaseLX Long Haul GBIC

This module provides a GBIC interface for SC-type fiber connectors. The interface supports 10 micron single mode fiber for distances up to 100 kilometers.

1000BaseLX GBIC

This module provides a GBIC interface for SC-type fiber connectors. The interface supports 10 micron single mode fiber for distances up to 5 kilometers.

Features

The following table lists the major features of the IntraCore 8000 switch.

Feature	Description
Media Flexibility	Expansion module options include 8-port 10/100 Base-TX switched Ethernet modules and single-port Gigabit Ethernet modules with GBIC slots.
High Density	Supports up to 192 10/100 switched Ethernet ports or up to 3 switched Gigabit Ethernet ports and 24 10/100 switched Ethernet ports in a single stacking unit. This saves space in crowded equipment rooms.
ASIC-Based Architecture	ASIC-based packet processing provides wire speed performance on all interfaces.
High Performance 16Gbps Backplane	The system supports current requirements for multi-service voice, video, and data applications with bandwidth to spare. The high-capacity backplane is designed so that it may be scaled up to 80 Gbps, extending the useful life of the chassis.
Multiple Priority Queues	The “application aware” system ensures that mission critical applications get the bandwidth and priority they need, even under heavy traffic conditions. When network congestion occurs, low latency requirements are managed by the system.
Stackable Form Factor with modular expansion options	Each stack unit supports three option slots that can be customized to meet customer configuration requirements. Unique stacking design delivers scalable system bandwidth assuring maximum system performance regardless of configuration.
Configuration Flexibility and Growth	Expansion modules can be mixed and matched in any configuration and quantity to meet design requirements. You can add capacity whenever your business requires it.
GBIC Modules for Gigabit Ethernet Media Flexibility	The two GBIC Gigabit Ethernet modules can be configured with any combination of 1000SX, 1000LX or 1000LX (Long Haul) GBIC interfaces. Either Asanté or third party GBIC interfaces can be used, and the interfaces can be “hot swapped.” This means that GBIC interfaces can be re-deployed based on the user’s applications.
Installation Options	The system can be rack-mounted to save space.

Feature (Cont.)	Description (Cont.)
Security	Node summary tracks MAC and IP addresses per device, for multiple devices on each port. The Port Security feature provides per-port security, allowing the network manager to specify which MAC is authorized on each port. Only the device with that MAC address is allowed to connect to that specific port.
Web Based Management	Built-in Web-based interface is provided for chassis management, module management, port-level control, and monitoring. The IntraCore 8000 can also be managed via Telnet, Console, or third party SNMP console.
VLANs	Supports up to 64 port-based VLANs (IEEE 802.1Q compliant) for security, logical network design, and the control of broadcast traffic. The 802.1Q standard specifies VLAN tagging for trunking VLANs from switch to switch, or switch to router. Compatible with all 802.1Q equipment for easy integration into existing networks.
Multicast Control	The IntraCore 8000 supports standards based IGMP snooping and GMRP for control of multicast traffic generated by bandwidth-hungry applications such as video, ensuring maximum application and network performance.
RMON	The administrator can use an RMON probe for in-depth traffic analysis, with support for four groups of RMON.
Spanning Tree Protocol	Spanning Tree Protocol (STP) detects and eliminates data loops to prevent broadcast storms from overwhelming your network.
Y2K compliance	All IntraCore 8000 modules are Y2K compliant.

Table 1-2 IntraCore 8000 Features

Defaults and Specifications

The IntraCore 8000 is shipped with the following factory default settings and specifications:

Configuration	Default Setting
Backplane Speed	16Gbps/stack unit, up to 80Gbps in a 4 unit stack.
Switching Method	Store-and-forward
Forwarding Rates: (64 byte packets)	Switched 10Mbps = 14,880 pps Switched 100Mbps = 148,810 pps Switched 1000Mbps = 1,488,100 pps
Buffer Size	4MB
MAC Address Table	8K
Full-Duplex	Standards based Auto-negotiation enabled
VLAN	64 port-based VLANs, GVRP support, 802.1Q VLAN Tagging
Spanning Tree Protocol	802.1D, enabled
Flood Rate Limiting	Broadcast/multicast traffic
Priority	802.1p, 8 levels mapped to 4 queues
RMON	Groups 1-3, 9
SNMP	MIB-II, Bridge MIB, RMON MIB, Asanté private MIBs
Console Baud Rate	9600
Password	Asante

Table 1-3 Defaults and Specifications

LEDs

The following indicator lights are used on the various modules of the IntraCore 8000.

LED	Color and Meaning
Stacking (to left of modules)	
Power	Green - Power is on when lit
Stack Number	Specifies IntraCore 8000 Unit – #1 is bottom unit
Stack CPU	Specifies IntraCore 8000 unit with management CPU
Matrix Board Present	Indicates whether or not current unit has the Matrix module for the other units in the stack
MII Present	Indicates whether or not a Media Independent Interface module has been installed in the current IntraCore 8000 unit
8-port 10/100 Switch Module	
Link/Speed	Green - Connection and link have been made
Duplex/Activity	Green -Full Duplex Amber - Half Duplex Blinking - Active
Gigabit Switch Module	
Power	Green - Power is on when lit
Link	Green - Connection and link have been made.

Table 1-4 LEDs and their meanings

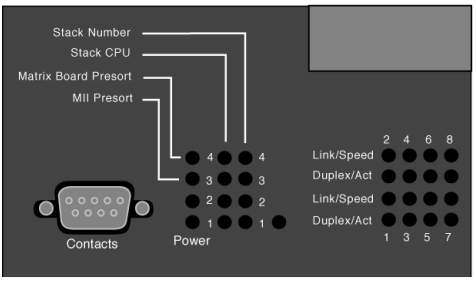


Figure 1-4 LEDs on face plate

2
Installation and Setup

This chapter explains how to install, connect, and configure the IntraCore 8000 chassis and modules to work with your network. It also explains how to set up your IntraCore 8000 for management, either from a console, via telnet, via SNMP, or by using a Web browser.

Installation Guidelines

The following guidelines will help you prepare to install your IntraCore 8000 in such a way that it has the proper power supply and environment.

Power Requirements

The source electrical outlet should be installed near the IntraCore 8000 and easily accessible. It must also be properly grounded.

Make sure the power source adheres to the following guidelines:

- ❑ Voltage range: 100 to 240 VAC
- ❑ Frequency range: 60/50 Hz
- ❑ Maximum current: 3.5 A per power supply at 110 volts

Environmental Requirements

The IntraCore 8000 must be installed in a clean, dry, dust-free area with adequate air circulation to maintain the following environmental limits:

- ❑ Temperature: 0° to 40° C (32° to 104° F)104°
- ❑ Relative Humidity: 5% to 85% non-condensing

Avoid direct sunlight, heat sources, or areas with high levels of electromagnetic interference.

Cooling and Airflow

Do not restrict air flow by covering or obstructing air vents on the sides of the IntraCore 8000.

Installation Overview

The table below describes the steps needed to install the IntraCore 8000. The steps that are optional are labeled “optional” and the steps that are required are labeled “required.” The sections that follow explain each step in detail.

Step	Action to Be Taken
1 (Required)	Open the box and check the contents. See the Package Contents sheet for a complete list of the items included with your IntraCore 8000.
2 (Required)	Install the IntraCore 8000 chassis in an equipment rack or wall rack, or prepare it for desktop placement. See page 2-3.
3 (Optional)	Create a stack of up to four IntraCore 8000 switches. See page 2-5.
4 (Optional)	Install the port expansion modules you have purchased for your IntraCore 8000 and ensure each is properly seated and locked in place. See page 2-7.
5 (Required)	Connect the power supply. See page 2-9.
6 (Required)	Connect network devices to the IntraCore 8000. See page 2-10.
7 (Required)	Configure the IntraCore 8000 for management capabilities. See page 2-11.

Table 2-1 Installation Overview

Chassis Installation/Placement

The IntraCore 8000 can be installed in a standard 19-inch equipment rack. It can also be placed on a stable horizontal surface.

▲ Important: The equipment rack or desk on which you install your IntraCore 8000 *must* be secure and stable. Equipment racks must be fastened to the floor; desks must be resting on a flat, stable surface.

Installation in an Equipment Rack

To install the unit in an equipment rack, use the following procedure.

Safety Precautions for Rack Installation

▲ Important! Before continuing, disconnect all cables from the IntraCore 8000. Also, do not install any optional modules you have purchased until the switch has been installed in the rack.

Equipment Rack Guidelines

Guideline	Specification
Size	Width; 17.75 inches (45.09 cm). Depth: 19.25 inches (48.9 cm) to 32 inches (81.3 cm).
Stability	Rack must be bolted to the floor. Mount heavier units at the bottom of the rack. If the IntraCore 8000 is the only unit, mount it the bottom of the rack..
Ventilation	Ensure that the rack is installed in a room where the temperature remains below 40° C (104° F). Ensure also that there are no obstructions, such as other equipment or cables, blocking airflow to or from the IntraCore 8000 vents.
Clearance	In addition to providing clearance for ventilation, ensure that there is adequate clearance for servicing the modules of the IntraCore 8000 from the front.

Table 2-2 Equipment Rack Guidelines

Equipment Rack Installation Procedure

To mount the IntraCore 8000 in an equipment rack:

1. Place the IntraCore 8000 on a flat, stable surface.
2. Locate a rack-mounting bracket (supplied) and place it over the mounting holes on one side of the unit.
3. Insert six screws (supplied) into the holes and tighten with a Phillips screwdriver. Do not use fewer than six screws for this mounting.
4. For the other side of the unit, repeat the two previous steps.
5. Place the unit in the equipment rack.
6. Secure the unit by screwing its mounting brackets to the equipment rack. Use a minimum of four screws for this purpose.

   ▲ Important! Make sure the unit is supported until all the mounting screws for each bracket are secured to the equipment rack. Failure to do so could cause the unit to fall, resulting in personal injury or damage to the unit, or both.

7. Proceed to the section, “Installing Port Expansion Modules.”

Free-Standing/Desktop Placement

The IntraCore 8000 has four rubber feet on the bottom of the case that allow for free-standing placement of the unit.

For free-standing/desktop placement:

1. Attach the four rubber pads (supplied) to the bottom of each corner of the IntraCore 8000 chassis.
2. Place the unit on a flat surface with a minimum area of 17.1” x 13.5” (434.3 mm x 342.9 mm) and support capacity of 22 lbs (10 kg).
3. Make sure there is enough ventilation space between the IntraCore 8000 and surrounding objects.

Stacking Switches

Up to four IntraCore 8000 switches may be connected within a stack. In each of the different configurations, bandwidth increases to meet the growth of traffic.

Two Stack Configuration

If you wish to add a single switch to create a stack of two, take the following steps.

1. Mount the second switch in the rack above the first switch, or place it on top of the first switch.
2. Connect the 20-pin stacking cable provided by Asanté from the Stack Connector module on the back of the first switch to the Stack Connector module on the second switch.
   - *Note:* Do not use any cable but the IntraCore 8000 stacking cable supplied with your unit. If you need additional cables, contact Asanté support (see Appendix A, "Technical Support," for details).

Three or Four Stack Configuration

Before stacking three or four IntraCore 8000 switches, you must obtain a Stack Matrix module from Asanté. IntraCore 8000 switches come equipped with a single-port Stack Connector module. On one of the switches, the Stack Connector module must be replaced with a 3-port Stack Matrix module.

To create a stack of three or four IntraCore 8000 switches, use the following procedure.

1. In the original switch (bottom), remove the (single-port) Stack Connector module from the back of the switch and replace it with a (3-port) Stack Matrix module.
2. Mount the other switches in the rack above the first one, or place them on top of the first switch.

3 Connect the Stack Matrix module on the first switch to the Stack Connector modules on the other switches. Use the 50-pin stacking cables provided by Asanté, as shown in Figure 2-1.

- *Note:* Do not use any cable but the IntraCore 8000 stacking cable supplied with your unit. If you need additional cables, contact Asanté support (see Appendix A, "Technical Support," for details).

Figure 2-1 Four stack configuration

When you have cabled the switches together, proceed with network cabling, as described in "Connecting to the Network" earlier in this chapter.

Installing Port Expansion Modules

Up to three optional port expansion modules can be installed in the IntraCore 8000, in addition to a stack matrix module. (A stack matrix module is needed only if more than two units are stacked together. See “Stacking Switches.”)

To install any combination of Gigabit Ethernet Switch (GBIC) modules and 8-port 10/100 Switch modules, use the following procedure.

▲ Important: Make sure the IntraCore 8000 is properly installed in an equipment rack or resting on a flat, stable surface. Also make sure the power cord is disconnected for initial installation.

1 Remove the cover plate from the slot where you intend to install the expansion module.

2 Align the bottom of the expansion module with the rails inside the IntraCore 8000 slot, as shown in Figure 2-2.

3 Slide the module into the slot until it stops, then push the module in gently until it seats with the connector.

Figure 2-2 Installing port expansion module

4 Tighten the thumbscrews at the ends of the module’s face plate. Use a straight-bladed screwdriver so the thumb-screws cannot be loosened by hand.

Installation of the module is complete. Repeat this procedure for each module you have purchased.

▲ **Important:** Do not remove modules from the IntraCore 8000 unless you are a qualified System Administrator.

Installing GBIC Interfaces

If you have installed Gigabit Ethernet switch modules, you must install GBIC interfaces. Instructions for installing, removing, and maintaining GBIC interfaces are provided in this section.

- *Note:* GBICs are hot-swappable.

Installing a GBIC

To install a GBIC interface into a Gigabit Ethernet module:

1. Remove the GBIC from its protective packaging.
2. Grip the sides of the GBIC with your thumb and forefinger, then insert the GBIC into the slot on the front of the Gigabit Ethernet module.
3. Slide the GBIC into the slot until you hear or feel a click. The click indicates that the GBIC is locked into the slot.
4. When you are ready to attach the fiber-optic cable, remove the plugs from the GBIC and save them for future use.

Removing a GBIC

To remove a GBIC interface from a Gigabit Ethernet module:

1. Disconnect the fiber-optic cable from the GBIC SC-type connector.
2. Release the GBIC from the slot by simultaneously squeezing the plastic tabs on both sides of the GBIC.
3. Slide the GBIC out of the slot.
4. Install the plugs in the GBIC optical bores, and place the GBIC in protective packaging.

GBIC Care and Handling

Follow these GBIC maintenance guidelines:

- ❑ Unnecessary removal and insertion of a GBIC can lead to its premature failure. A GBIC has a lifetime of 100 to 500 removals/insertions.
- ❑ GBICs are static-sensitive. To prevent ESD damage, follow your normal board and component handling procedures.
- ❑ GBICs are dust-sensitive. When the GBIC is stored or when a fiber-optic cable is not plugged in, always keep plugs in the GBIC optical bores.
- ❑ Use an alcohol swab or Kim-Wipe to clean the ferrules of the optical connector. The most common source of contaminants in the optical bores is debris picked up from the optical connectors.

Connecting Power

To connect power to the IntraCore 8000, use the following procedure.

▲ Important: Carefully review the power requirements on page 2-1 before connecting power to the IntraCore 8000.

1 Plug one end of the supplied power cord into the power connector on the back of the unit.

2 Plug the other end into a grounded AC outlet.

The front panel LEDs blink and the Power LED illuminates. The IntraCore 8000 is ready for connection to the network.

▲ Important: If the power does not come on, refer to Appendix A, “Troubleshooting.”

Connecting to the Network

The IntraCore 8000 unit may be connected to an Ethernet network, with the unit powered either on or off. Use the following procedure to make your network connections.

1. Connect network devices to the IntraCore 8000, following the cable guidelines outlined below.
2. After the unit is connected to the network, it can be configured for management capabilities. See "Configuring for Management" later in this chapter.

10/100BaseX Ports Cabling Procedures

The 8 fixed ports on each 10/100 module allow for the connection of 10Base-T or 100Base-TX network devices. The ports are compatible with IEEE 802.3 and 802.3u standards.

▲ Important: The IntraCore 8000 must be located within 100 meters of its attached 10Base-T or 100Base-TX devices.

Connecting To	Cable Required
Network Station	Category 5 UTP (Unshielded Twisted-Pair) straight-through cable (100 meters maximum) with RJ-45 connectors.
Repeater/Hub	Category 5, UTP cross-over cable (100 meters maximum) with RJ-45 connectors.
Repeater/Hub's Uplink port	Category 5, UTP straight-through cable (100 meters maximum) with RJ-45 connectors.

Table 2-3 10/100BaseTX cabling requirements

1000BaseX Ports Cabling Procedures

Cabling requirements for the 2-port Gigabit Ethernet modules depend on which type of GBIC interface has been installed. Use the following chart to determine the cabling requirements for your GBIC.

Connecting To	Cable Required
1000BaseSX GBIC	Cables with SC-type fiber connectors: 62.5 micron multimode fiber media up to 275 meters long, or 50 micron multimode fiber media up to 550 meters long.
1000BaseLX Long Haul GBIC	Cables with SC-type fiber connectors: 10 micron single mode fiber media up to 100 kilometers long.
1000BaseLX GBIC	Cables with SC-type fiber connectors: 10 micron single mode fiber media up to 5 kilometers long.

Table 2-4 1000BaseX cabling requirements

Configuring for Management

To use the IntraCore 8000 as a managed switch, it must be configured with an IP address. This can be accomplished in one of two ways:

- ❑ automatically using BootP (default)
- ❑ manually via the unit's Console port

▲ Important: For security reasons, you should also change the SNMP community strings before putting the IntraCore 8000 on your network. For instructions, see "Changing Community Strings" on page 3-17.

BootP Configuration

The IntraCore 8000 is shipped with BootP support. If your network contains a BootP server configured with available, valid IP addresses, BootP allows the IntraCore 8000 to be configured automatically with an IP address when the IntraCore 8000 is connected to the network and is powered on. Use the following procedure to set up BootP.

▲ Important: BootP configuration works only if the IntraCore 8000 does not have an IP address assigned to it.

1 Make sure your network has a BootP server configured with a valid IP address entry for the IntraCore 8000.

2. When the IntraCore 8000 is connected to the network and is powered on, it automatically transmits a BootP request across the network (up to 10 times) until it receives a valid IP address from the BootP server.
3. After an IP address is received, the IntraCore 8000 can be managed via in-band access. For more information, see Chapter 3, “Configuration.”

To verify that a valid IP address was received, try to ‘ping’ the IntraCore 8000. If you can access the IntraCore 8000, it is properly configured with an IP address.

For more information on using BootP, see “Bootstrap Configuration” in Chapter 3.

Connecting To a Console

To make the cable connection from a terminal to the console port of the IntraCore 8000, use the following procedure.

1. Using a straight-through RS-232 cable with a 9-pin male D-subminiature plug at one end, connect a terminal or workstation (PC or Macintosh) running a terminal emulator to the console port on the front of the IntraCore 8000.
2. Make sure both units are powered on.

   If using a PC with a terminal emulator, make sure it is configured with the following terminal settings:

   - ❑ Baud: 9600
   - ❑ Data Bits: 8
   - ❑ Parity: None
   - ❑ Stop Bits: 1
   - ❑ Flow Control: None
3. Once connected, the Local Management Main Menu appears on the terminal screen.

For further information on setting an IP address for configuration of a terminal, or a PC running a VT100 terminal or emulator (such as HyperTerminal, ProComm, or ZTerm), see “System IP Configuration” in Chapter 3.

Management Options

The IntraCore 8000 can be managed using any of the following methods:

Method	Type	Description
Console	Out-of-band management	Local connection to the IntraCore 8000 via the console port
Telnet (four sessions maximum)	In-band management	Remote connection over the network to the IntraCore 8000 via telnet session
HTTP Server	In-band management	Remote connection to the IntraCore 8000 via a Web browser
SNMP-Based Network Management Software	In-band management	Remote connection to the IntraCore 8000 via any SNMP-based network management application

Table 2-5 Management Methods

The rest of this section describes how to connect to the IntraCore 8000 using either out-of-band or in-band management.

Out-of-Band Management

Out-of-band network management allows you to configure, manage, and monitor the IntraCore 8000 and all of the installed modules. You can perform these functions by attaching a terminal (or a terminal emulator) to the Console port on the management engine and using the menu-driven Local Management Interface.

Out-of-band network management is guaranteed even when the in-band Ethernet network is down.

To access the IntraCore 8000 Local Management Interface using out-of-band management, first follow the procedure in “Connecting To a Console” (above), then go on to the “Local Management Interface” section in Chapter 3.

In-Band Management

In-band network management allows you to configure, manage, and monitor the IntraCore 8000 over the Ethernet network.

You can perform these functions by accessing the IntraCore 8000 via any of the following methods:

- ❑ By connecting with a telnet program and using the Local Management Interface.
- ❑ By connecting with any World Wide Web browser, and using the Web Management Interface.
- ❑ By connecting with any SNMP-based network management application and using its interface.

To manage the IntraCore 8000 via in-band management, use the following procedure.

1. Make sure the network to which the IntraCore 8000 is connected is functioning.
2. Make sure the IntraCore 8000 is configured with valid IP information. See "Configuring for Management" earlier in this chapter.
3. Connect to the IntraCore 8000 via telnet, with a Web browser, or with any SNMP-based network management application.

Telnet

Use a network connection to any PC and enter the **`telnet`** command to access the IntraCore 8000. The password prompt of the Local Management Interface will appear. Go on to the "Local Management Interface" section in Chapter 3.

- ◆ *Note:* Almost all management screens using a telnet connection are identical to those of the out-of-band console interface. On the Main Menu, however, there will be a q option for closing the connection to the IntraCore 8000.

Web Browser

For information on managing the IntraCore 8000 with a Web browser, refer to Chapter 5, “Web Browser Management.”

- *Note:* The Web Browser interface to the IntraCore 8000 is disabled by default.

SNMP-Based Management

For information on managing the IntraCore 8000 with SNMP-based management software, refer to Chapter 4, “Advanced Management,” and your SNMP software manual.

The Asanté private MIB for the IntraCore 8000 is available from the Asanté ftp site, *ftp.asante.com*, or you can copy it from the Installation CD-ROM.

Access to Remote Network Monitoring (RMON) features is available only by using an SNMP manager. See “SNMP and RMON Management” in Chapter 4 for details.

3
Configuration

This chapter describes how to manage the IntraCore 8000 using the Local Management Interface via an out-of-band console connection or an in-band telnet connection.

This chapter contains the following sections:

- Local Management Interface
- Viewing General Information
- Configuration Menu
- System Administration Configuration
- System IP Configuration
- Bootstrap Configuration
- SNMP Configuration
- Port Configuration
- Advanced Port Configuration
- Global Port Configuration
- Unicast Forwarding Database Configuration
- Image File Downloading Configuration
- Stack Management
- System Reset Configuration
- Viewing the System Log
- User Interface Configuration
- Viewing Statistics

Local Management Interface

The IntraCore 8000 Local Management Interface is a menu-driven application that allows you to configure, manage, and monitor the IntraCore 8000 and each of the ports in its different modules.

The Local Management Interface can be accessed via two methods:

- ❑ Out-of-band connection to the Console port
- ❑ In-band connection via Telnet (*four* sessions maximum)

For instructions on how to connect to the IntraCore 8000, see "Management Options" on page 2-13.

The rest of this chapter describes the Local Management Interface.

Logging In

When you connect to the Local Management Interface, the "Enter Password" prompt appears. Enter your password, then press **Return**. The Main Menu appears.

▲ Important: The default password is **Asante**. The password is case-sensitive; enter it exactly as shown. For information on changing the password, see "Changing the Password" on page 3-51.

Main Menu

After logging in, the Main Menu appears, as shown in Figure 3-1.

```
================================================================
IntraCore 8000  Local Management System Version 1.02D
Compiled Date: Jun 23 2000 19:53:29
Asante Technologies, Inc.
Copyright (c) 1999 Asante Technologies, Inc.
================================================================

Main Menu

<Cmd>           <Description>
  g              General Information
  c              Configuration
  s              Statistics
  q              Return to previous menu


Command>
```

Figure 3-1 Local Management Main Menu

From the Main Menu, you can access three submenus:

- ❑ General Information (see page 3-4)
- ❑ Configuration (see most of this chapter)
- ❑ Statistics (see page 4-1)

If you are using Telnet, a fourth option, for closing the connection, will also be available.

Accessing a Submenu

To access a submenu, type the command letter that corresponds with the option you need to use. For example, type g for General Information.

Exiting a Submenu

To exit a submenu, type q.

To exit a command line without changing the configuration setting (e.g., the "Set Password" option in the User Interface Configuration Menu), press **ctrl-c**.

Viewing General Information

The General Information Screen displays the current operating information of the IntraCore 8000, such as its name, IP address, and boot information.

To view General Information, type **g** from the Main Menu. A screen similar to Figure 3-2 appears.

```
IntraCore 8000  General Information

System up for:  000days, 21hrs, 45mins, 45secs
Software Version
   Bank 1 Image Version/Date:     1.10/Dec  7 1999 12:14:38 (Running)
   Bank 2 Image Version/Date:     1.10/Dec  7 1999 11:54:14
System Information
   Prom Image Ver/Date:           1.01/Sep  8 1999 15:59:14
   DRAM Size:           4MB        Flash Size:             2.0MB
   EEPROM Size:         32KB       Console Baud Rate:      9600 bps
Administration Information
   System Name:         Asante IntraCore Switch
   System Location:     ZLabs Head Office
   System Contact:      CLB
System MAC Address, IP Address, Subnet Mask and Router
   MAC Address:         00:00:94:8E:F3:7B
   IP Address:          192.168.54.240
   Subnet Mask:         255.255.255.0
   Router:              192.168.54.2
Bootstrap Configuration
   Boot Load Mode:      LOCAL

Press any key to continue...
```

Figure 3-2 General Information screen

- *Note:* The information displayed on this screen is read-only.

To exit the General Information Screen, press any key on your keyboard.

Table 3-1 describes each parameter in the General Information screen.

Setting	Description
System Up Time	The amount of time the system has been running since last reset or power on.
Bank 1 Image Version/ Date	The version and compilation date of the runtime code that is stored in Bank 1. (Running) indicates code is currently active.
Bank 2 Image Version/ Date	The version and compilation date of the runtime code that is stored in Bank 2.
Prom Image Ver/Date	The version and compilation date of the PROM.
DRAM Size	The size in megabytes (MB) of the unit's Dynamic Random Access Memory.
EEPROM Size	The size in megabytes (MB) of the unit's EEPROM.
Flash Size	The size, in MB, of the switch's flash memory, or non-volatile RAM.
Console Baud Rate	The current rate which data transfers to the console from the IntraCore 8000.
System Name	The name assigned to the IntraCore for network purposes.
System Location	The physical location of the IntraCore.
System Contact	Person responsible for configuration of the unit.
MAC Address	The hardware address of the IntraCore 8000; this address cannot be changed
IP Address	The unit's IP (Internet Protocol) address.
Subnet Mask	The IP subnet mask for the IntraCore 8000.
Router	The IP address of the default gateway router to which the switch belongs.
Boot Load Mode	The current method in use for loading the switch's software.

Table 3-1 General Information settings

Configuration Menu

The Configuration Menu allows you to manage and configure the IntraCore 8000 and each of its ports.

To access the Configuration Menu, type **c** from the Main Menu. The Configuration Menu appears, as shown in Figure 3-3.

```
IntraCore 8000  Configuration Menu

<Cmd>          <Description>
  a            System Administration Configuration
  i            System IP Configuration
  b            Bootstrap Configuration
  n            SNMP Configuration
  p            Port Configuration
  s            Spanning Tree Configuration
  d            Unicast Forwarding Database Configuration
  t            Security Management
  v            VLAN Management
  c            Multicast Traffic Management
  f            File Downloading Configuration
  k            Stack management
  r            System Reset Options
  l            System Log
  u            User Interface Configuration
  q            Return to previous Menu


Command>
```

Figure 3-3 Configuration Menu

Accessing a Submenu

To access a submenu, type the command letter that corresponds with the configuration option you need to use. For example, type a for the System Administration Configuration Menu.

Configuration Menu Options

Table 3-2 describes each of the options in the Configuration Menu.

Menu Item	Description
System Administration Configuration	Displays and allows you to change the name, location, and contact information for the IntraCore 8000. See page 3-8.
System IP Configuration	Displays and allows changing the IP Address of the IntraCore 8000. This address is for network access to the switch. See page 3-9.

Menu Item (Cont.)	Description (Cont.)
Bootstrap Configuration	Allows you to change boot bank and method for loading switch software, or change downloading parameters. See page 3-11.
SNMP Configuration	Displays and allows you to change the SNMP (Simple Network Management Protocol) parameters of the IntraCore 8000; such as read/write community strings. See page 3-16.
Port Configuration	Allows you to configure manually each of the switch's ports for speed, connection, link mode, and auto-negotiation. Also displays overall port status. See page 3-19.
Spanning Tree Configuration	Displays and allows you to change Spanning Tree parameters, to make sure you prevent loops in network paths. See page 4-1.
Unicast Forwarding Database Configuration	Allows you to display all of the forwarding database, or display it by port or VLAN, either with or without showing IP addresses. Also lets you search for MAC or IP addresses and lets you set the age-out time for MAC addresses. See page 3-33.
Security Management	Allows you to use various features such as Duplicate IP traps, for port security. See page 4-9.
VLAN Management	Allows you to set up virtual networks. See page 4-18.
Multicast Traffic Management	Allows you to set up group transmission. See page 4-44.
File Downloading Configuration	Allows you to download an image file for the purpose of upgrading the IntraCore 8000 software. See page 3-38.
Stack Management	This feature is undocumented.
System Reset Options	Allows you to reset the switch by a "warm" reboot, or arrange for an automatic reset (up to 24 hours) in advance. See page 3-45.
System Log	Allows you to view a record of any major system events or errors that have occurred on the IntraCore 8000. See page 3-47
User Interface Configuration	Allows you to set the idle time-out period and password when using console or telnet access. See page 3-49.
Return to Previous Menu	Allows you to exit the Configuration Menu and return to the Main Menu.

Table 3-2 Configuration Menu Options

Most of the options for configuration are described in detail in the rest of this chapter. The more advanced options are discussed in Chapter 4, "Advanced Management."

System Administration Configuration

The System Administration Configuration Menu displays and allows you to change the IntraCore 8000's name, location, and contact information.

To access the System Administration Configuration Menu, type **a** in the Configuration Menu. A screen similar to Figure 3-4 appears.

```
IntraCore 8000  System Admin. Configuration Menu

System Name:          Asante IntraCore Switch
System Location:      ZLabs Main Office
System Contact:       CLB

<Cmd>       <Description>
  n         Set System Name
  l         Set System Location
  c         Set System Contact Information
  q         Return to Previous Menu

Command>
```

Figure 3-4 System Administration Configuration Menu

Current Settings

The following table describes each setting on the System Administration Configuration Menu.

Setting	Description
System Name	The name of the IntraCore 8000 (up to 64 characters, including spaces).
System Location	Place where you have installed the IntraCore 8000 (up to 64 characters, including spaces).
System Contact	The name of the person or entity responsible for the IntraCore 8000 (up to 64 characters, including spaces).

Table 3-3 System Administration settings

Changing System Administration Info

To change the name, location, or contact information for the IntraCore 8000, use the following procedure.

1. Open the System Administration Configuration Menu by typing a in the Configuration Menu.
2. Type the command letter of the item to be changed in the System Administration Configuration Menu.
3. At the prompt, type the information you want to change.

   See Table 3-3 for a description of each parameter.

   - *Note:* Each parameter is limited to 64 characters, including spaces.

   To cancel a selected option, press ctrl-c at the command prompt.
4. Press Return.

   The IntraCore 8000 system administration information changes take effect.
5. Type q to quit and return to the Configuration Menu.

System IP Configuration

The System IP Configuration Menu displays and allows you to change the information needed to access the IntraCore 8000 over the network via in-band management.

To access the System IP Configuration Menu, type i in the Configuration Menu. A screen similar to Figure 3-5 appears.

```
IntraCore 8000  System IP Configuration Menu

System MAC Address:          00:00:92:CC:BB:AA
System IP Address:           192.168.54.240
System Subnet Mask:          255.255.255.0
System Default Router:       192.168.54.2

<Cmd>      <Description>
  i        Set IP Address
  m        Set Subnet Mask
  r        Set Default Router
  n        Set Domain Name Server
  q        Return to Previous Menu

Command>
```

Figure 3-5 System IP Configuration Menu

▲ Important: By default, each address is set to 0.0.0.0.

Current Settings

Table 3-4 describes each setting on the System IP Configuration Menu.

Setting	Description
System IP Address	The IP (Internet Protocol) address of the IntraCore 8000.
System Subnet Mask	The filter that determines how the IntraCore 8000 IP address is split into network and host portions.
System Default Router	The IP address of the default router for the IntraCore 8000.

Table 3-4 System IP settings

Changing System IP Information

To change the IP address, subnet mask, or default router of the IntraCore 8000, use the following procedure.

1. Open the System IP Configuration Menu by typing i in the Configuration Menu.
2. Type the command letter of the option you want to change.
3. Type the new address at the prompt.

   See Table 3-4 for a description of each address.

   ▲ Important: Follow the format:

   number.number.number.number

   To cancel a change, press ctrl-c at the command prompt.
4. Press Return.

   The IP setting change for the IntraCore 8000 takes effect.
5. Type q to quit and return to the Configuration Menu.

Bootstrap Configuration

The Bootstrap Configuration Menu displays (and allows you to change) the bootstrap parameters used for loading the software for the IntraCore 8000 at startup, and for downloading a new version of software when one is issued.

To access the Bootstrap Configuration Menu, type b in the Configuration Menu. If the Load Mode is set to Local, a screen similar to Figure 3-6 appears.

```
IntraCore 8000 Bootstrap Configuration Menu

Bank 1 Image Version/Date:      1.00B/May 3 1999 10:00:07  (Running)
Bank 2 Image Version/Date:      1.00G/May 5 1999 17:32:18

Load Mode:    Local
Boot Bank:    2

<Cmd>       <Description>
  r         Set Load Mode to REMOTE
  a         Toggle Boot Bank
  q         Return to previous menu

Command>
```

Figure 3-6 Local Bootstrap Configuration Menu

When the IntraCore 8000 is powered on, it loads its software via one of two methods: locally (via its internal flash memory, which is the default setting) or remotely over the network.

▲ Important: The default Load Mode setting for the IntraCore 8000 is Local.

Image Banks

The IntraCore 8000 has two banks to store its runtime software. The banks are referred to as bank 1 and bank 2.

Either of these banks may be the Boot Bank, which is the bank from which the runtime code will be loaded the next time the IntraCore 8000 is booted.

When downloading new runtime image codes, you may specify either of the two banks as the Destination Bank in which the new code will be loaded.

Loading Software Locally

The IntraCore 8000 will always boot locally unless you set it to boot load remotely. It would then download the new image code and reset to load locally.

1. Open the Bootstrap Configuration Menu by typing b in the Configuration Menu.
2. Type a in the Bootstrap Configuration Menu if you need to toggle the Boot Bank setting for the next boot. Typically, you will want to set the boot bank to be the one on which the latest version of the Image resides.

The IntraCore 8000 is set to load software locally from its flash memory. This occurs whenever the unit is powered on or reset.

Loading Software Remotely

To set the IntraCore 8000 to download its software over the network from a remote server, use the following procedure.

1. Open the Local Bootstrap Configuration Menu by typing b in Configuration Menu.
2. Open the Remote Bootstrap Configuration Menu by typing r in the Local Bootstrap Configuration Menu. The menu appears, as shown in Figure 3-7.

```
IntraCore 8000  Bootstrap Configuration Menu

Bank 1 Image Version/Date:     1.10J/Dec 7 1999 12:14:38  (Running)
Bank 2 Image Version/Date:     1.00G/May 5 1999 17:32:18

Load Mode:          Remote
Boot Mode:          TFTP only
Boot Server IP:     192.168.54.150
Boot File Name:     c:\base\newcrc.ima
Retry Count:        5
Boot Bank:          1

<Cmd>       <Description>
  b          Set Boot Mode to BOOTP-TFTP
  t          Set Boot Mode to TFTP only
  l          Set Load Mode to LOCAL
  s          Set Boot Server IP Address
  f          Set Boot File Name
  c          Set Remote Boot Retry Count
  a          Toggle Boot Bank
  q          Return to Previous Menu

Command>
```

Figure 3-7 Remote Bootstrap Configuration Menu

Current Settings

Table 3-5 explains each setting on the Remote Bootstrap Configuration Menu.

Setting	Description
Running Image Version/ Date	The version and compilation date of runtime code that is currently running on the IntraCore 8000.
Load Mode	The current method for loading software for the IntraCore 8000. Remote — Loads the image file from a server on the network. Local — Executes the software image file from the IntraCore 8000's internal flash memory (default setting; the IntraCore 8000 automatically reverts to this setting after downloading a new software file).
Boot Mode	The method for requesting the image file from the network. This option is available only if you have selected Remote Load Mode. BootP-TFTP — Sets the IntraCore 8000 to request an IP address from a BootP server AND to download the software's image file through TFTP (Trivial File Transfer Protocol). ▲ Important: To use this option, the IntraCore 8000 IP address must be set to 0.0.0.0. TFTP ONLY — Sets the IntraCore 8000 to only download the software image file through TFTP. ▲ Important: To use this option, the switch must already have an assigned IP address and the Load Mode must be set to Remote.
Boot Server IP	The Internet Protocol (IP) address of the TFTP server providing the TFTP capabilities on your network. Not Available if Boot Mode is BootP-TFTP.
Boot File Name	The name of the file you are going to request for download. Not available if boot mode is BootP/TFTP.
Retry Count	Number of attempts the IntraCore 8000 makes to download the image file if errors occur. The default is 5.
Boot Bank	Number of the destination bank for the image file you are downloading (1 or 2).

Table 3-5 Bootstrap Settings

3. Type b to set the Boot Mode to BootP-TFTP, or type t to set Boot Mode to TFTP only. If you choose BootP-TFTP mode, the options for setting the IP Address of the TFTP server and the Boot File Name become unavailable; in this case, skip Steps 4-7 and go on to Step 8.
4. Type s in the Bootstrap Configuration Menu, to select the option Set Boot Server IP Address.
5. At the prompt, type the IP address of the remote boot server that contains the switch's software image file. Then press Return. The Bootstrap Configuration Menu appears.
6. Type f to select the option Set Boot File Name.
7. Type the software's file name/network path at the prompt.
8. Press Return.

   - *Note:* If you decide to use Local Load Mode rather than Remote, type l. The Local Bootstrap Configuration Menu appears, as shown in Figure 3-6.

The IntraCore 8000 is now set to download its software remotely from the network. This will occur the next time the unit is powered on or reset.

SNMP Configuration

The SNMP Configuration Menu allows you to configure the unit's read and write community strings, and to enable or disable authentication traps. This menu also allows you to specify which of your network management stations will receive traps from the IntraCore 8000.

The s option in the Configuration Menu displays the SNMP (Simple Network Management Protocol) Configuration Menu, as shown in Figure 3-8.

For further details on using SNMP and RMON for remote management of your network, see Chapter 4, "Advanced Management."

▲ Important: Be sure to change the SNMP community strings in order to prevent unauthorized access to management information.

```
IntraCore 8000  SNMP Configuration Menu

SNMP Read Community:      public
SNMP Write Community:     private
Authentication Trap:      Enabled

SNMP Trap Receivers:
     IP Address           Community
1. 192.168.54.150         private
2. 192.168.54.110         Sarah
3. <EMPTY>                <EMPTY>
4. <EMPTY>                <EMPTY>

<Cmd>       <Description>
  r         Set SNMP Read Community
  w         Set SNMP Write Communtiy
  t         Toggle Trap Authentication Enable/Disable
  a         Add/Update SNMP Trap Receiver
  d         Delete SNMP Trap Receiver
  q         Return to Previous Menu

Command>
```

Figure 3-8 SNMP Configuration Menu

Current Settings

Table 3-6 describes each setting on the SNMP Configuration Menu.

Setting	Description
SNMP Read Community	The string that defines access rights for reading SNMP data objects. The default is public.
SNMP Write Community	The string that defines access rights for writing SNMP data objects. The default is private.
Trap Authentication	The status of the SNMP agent for authentication trap generation. The default is disabled.
SNMP Trap Receivers	The IP addresses of the network management stations that can receive traps from the IntraCore 8000. Normally, these addresses are the same as your network management software systems' IP addresses. ▲ Important: A maximum of four trap receivers is allowed.

Table 3-6 SNMP Settings

Changing Community Strings

To change the IntraCore 8000 community strings, use the following procedure.

1. Open the SNMP Configuration Menu by typing n in the Configuration Menu.
2. To change the read community string, type r. To change the write community string, type **w**.
3. At the prompt, type a new community string.

   For a description of read and write community strings, see Table 3-6.

   To cancel a selected option, press ctrl-c at the command prompt.
4. Press Return. The new string takes effect.
5. Type q to quit and return to the Configuration Menu.

Enabling Authentication Traps

The IntraCore 8000 can be set to generate authentication traps. Authentication traps are messages sent across the network to an SNMP network management station. They alert you when someone attempts to read or change data without the proper community string.

To set the IntraCore 8000 to generate traps, use the following procedure.

1. Open the SNMP Configuration Menu by typing n in the Configuration Menu.
2. To toggle trap authentication to Enabled, type a.

   To cancel the change, press ctrl-c at the command prompt.
3. Press Return. The new setting takes effect.
4. Type q to quit and return to the Configuration Menu.

Adding or Updating a Trap Receiver

Trap receivers are network management stations designated to receive traps from the IntraCore 8000.

▲ Important: The maximum number of trap receivers that can be set is four.

To add or update a trap receiver entry, use the following procedure.

1. Open the SNMP Configuration Menu by typing n in the Configuration Menu.
2. Type a to Add a Trap Receiver. An IP prompt appears.
3. Type the new or updated IP address of the network management station you want to receive traps, then press Return.

   To cancel an entry, press ctrl-c at the command prompt.
4. Type the trap receiver's community string at the prompt for it, then press Return again.

   The trap receiver entry is added or updated. Type q to return to the Configuration Menu.

Deleting a Trap Receiver

Use the following procedure to delete a trap receiver you have previously designated.

1. Open the SNMP Configuration Menu by typing n in the Configuration Menu.
2. Type d to Delete a Trap Receiver. A prompt for the entry of the trap receiver appears.
3. Enter the number of the entry you want to delete (1,2,3, or 4) and press Return.

The trap receiver is deleted from the SNMP Trap Receivers list.

Port Configuration

The Port Configuration Menu allows you to manually configure each of the IntraCore 8000's ports for port speed, duplex, and auto-negotiation. It also provides an overview of the entire IntraCore 8000 system's port operating status.

To access the Port Configuration Menu, type p in the Configuration Menu. A System Module Map screen similar to Figure 3-9 appears.

```
System Module Map
=================

Please select one of the following slots

  Slot          Description (Module Type)
  ----          -------------------------------------
    1           24 10/100BaseTX ports Module (24-100TX)
    2           2 1000BaseX ports Module (2-GBIC)
    3           24 10/100BaseTX ports Module (24-100TX)
    4           2 1000BaseX ports Module (2-GBIC)
    5           <none>
    6           <none>
    7           <none>
    8           <none>
    9           <none>


Enter Module Number (1-8)>
```

Figure 3-9 System Module Map screen

Choose the module for which you want to see a Port Configuration Menu. If, for example, you chose slot 1, you would see a screen similar to Figure 3-10.

```
IntraCore 8000 Basic Port Configuration MenuModule Type: [24-100TX/RJ45]
Module: [1]             Port:  [01]
Operating Status:   +---+---  --------  --------  -XXXXXXX  XXXXXXXX
Auto Negotiation:   ********  ********  ********  -XXXXXXX  XXXXXXXX
Speed/Duplex:       HHHHFHHH  HHHHHHHH  HHHHHHHH  GXXXXXXX  XXXXXXXX

Port Status: Enabled            Link Status: Up (RJ45-TX)
Auto-Neg:    Enabled[ABCD]      Link Speed:  100 Mbps (Half Duplex)

<Cmd>      <Description>
  h        Help for legends
  t        Toggle Port Status Enable/Disable
  u        Toggle Auto-Negotiation/Manual
  l        Toggle 10M/100M bps Link Speed
  d        Toggle Half/Full Duplex
  o        Modify Auto-Negotiation Advertisement
  r        Restart Auto-Negotiation
  a        Advanced Port Configuration
  g        Global Port Configuration
  q        Return to Previous Menu

Command>

Select module  Next module  Prev module  Select port  Next port  Prev port
```

Figure 3-10 Port Configuration Menu for 10/100BaseTX modules

Viewing Legends for Configuration Settings

To see legends explaining the symbols used for both the Basic and Global Port Configuration Menu settings, type h. A screen appears, as shown in Figure 3-11.

```
Legends for port  status:                  Legends for port speed & duplex:

     X - Absent                                 f -   10 Mbps & full duplex
     - - Link down                              F -  100 Mbps & full duplex
     D - Disabled by Mgmt Action                h -   10 Mbps & half duplex
     d - Disabled by Security Violation         H -  100 Mbps & half duplex
     B - Blocking                               G - 1000 Mbps & full duplex
     S - Listening
     R - Learning                            Legends for port priority:
     + - Forwarding                          (The range is from 0 to 7)
                                                0 - priority 0 (lowest)
Legends for Enable/Disable State:               1 - priority 1
     - - Disabled                                  2 - priority 2
     * - Enabled                                   3 - priority 3
                                                4 - priority 4
Legends for Auto-Negotiation Advertisement:     5 - priority 5
                                                6 - priority 6
     A - 100Base-TX full duplex mode            7 - priority 7 (highest)
     B - 100Base-TX half duplex mode
     C - 10Base-T full duplex mode
     D - 10Base-T half duplex mode


Press any key to continue...
```

Figure 3-11 Legends for all Port Configuration Menus

Current Port Settings

The current module and port for which statistics are displayed is shown in the top right corner of the Port Configuration Menu. Table 3-7 describes each setting on the Port Configuration Menu.

Setting	Description
Module Number	The number of the module of which the selected port is a member.
Module Type	Code for the type of module: 24-100TX, or 2-GBIC: See Figure 3-9 for the full names of each module type.
Port Number	The number of the port for which parameters are shown.
Operating Status	This field displays status symbols for each of the current module's ports. For details, see the legend in Figure 3-11.
Auto Negotiation	This field displays disabled/enabled symbols for each of the current ports. For details, see the legend in Figure 3-11.
Link Speed/Duplex	This field displays speed/duplex setting symbols for each of the current ports. For details, see the legend in Figure 3-11.
Port Status	Tells whether the selected port is enabled or disabled.
Link Status	Tells whether the selected port's link is up or down. 'Up' indicates a network device is connected to the port. 'Down' indicates that either a device isn't connected or that the device is powered down. The port's link speed and duplex mode are in parentheses.
Auto-Neg	Tells whether auto-negotiation is enabled or disabled for the selected port, and for which modes, A, B, C, or D. For details, see the legend in Figure 3-11.
Link Speed	Tells the speed and duplex mode of the port's current link.

Table 3-7 Port Configuration Menu settings

Enabling or Disabling a Port

The enabling or disabling of a port is a manual operation that can be used to isolate network devices possibly causing problems on the network or to prevent unauthorized use of a port or station.

To enable or disable a port, use the following procedure.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. To select the port you want to enable or disable, type s, n, or p in the Basic Port Configuration Menu.
4. To toggle the port's connection to either enabled or disabled status, type t.

The port's status is changed immediately, and it is reflected in the Port Configuration Menu's Port Status indication and the Operating Status symbol for the port.

Configuring Auto-Negotiation

Auto-negotiation is a feature of the Fast Ethernet standard that enables two devices on a common segment to communicate their transmission speed capabilities. This feature allows the devices to determine and use their highest common speed and best communication parameters.

▲ Important: By default, all of the ports are set to Auto Negotiation, as shown in Figure 3-10.

To enable auto-negotiation, or return to manual-setting mode, use the following procedure.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. To select the port for which you want to set the auto-negotiation mode, in the Basic Port Configuration Menu, type
   s, n, or p.
4. To toggle the port's auto-negotiation mode to Enabled or to return it to Manual, type u.

The Auto Negotiation status changes immediately, and is displayed on the Auto Negotiation line near the top of the Port Configuration Menu.

▲ Important: If you change the status of the port from Manual to Enabled you must type r to restart auto-negotiation.

Configuring a Port Manually

If you have changed the Auto Negotiation status of a port to Manual, as described in the previous section, you can toggle the link speed from 10Mbps to 100Mbps and back, and toggle the port from half to full duplex and back.

Toggling Port Link Speed

Use the following procedure to toggle the port's link speed.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. To select the port for which you want to set the link speed, in the Basic Port Configuration Menu, type s, n, or p.
4. To toggle the port's link speed, type l.

The link speed is changed immediately, and the change is reflected in the Link Speed line near the top of the Port Configuration Menu.

Toggling Half to Full Duplex

Half duplex mode allows transmission in two directions on the same channel, but only in one direction at a time. Full duplex mode allows transmission in two directions on the same channel at the same time.

▲ Important: To use full duplex mode, the device to which the port is connected must support and be configured for duplex mode.

Use the following procedure to change the duplex mode setting for a port that is in Manual status.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. To select the port for which you want to set the duplex mode, in the Basic Port Configuration Menu, type s, n, or p.
4. To toggle the port's duplex mode, type d.

The duplex mode is changed immediately, and the change is reflected in the Link Speed/Duplex line near the top of the Port Configuration Menu.

Configuring 1000BaseX Ports

Because 1000BaseX ports are always in full duplex mode, the only configuration option for 1000BaseX ports is enabling and disabling the port.

To access the Port Configuration Menu for 1000BaseX ports, type p in the Configuration Menu. The System Module Map appears, as shown in Figure 3-9. Enter the number of a module with 1000BaseX ports (such as module 2 in the map shown in Figure 3-9). The Port Configuration Menu for 1000BaseX ports appears, as shown in Figure 3-12.

```
IntraCore 8000 Basic Port Configuration Menu       Module Type: (2-GBIC)
Module: [1]                Port:   [1]
                        Port 1                     Port 2
                        ===========                ===========
Operating Status:       SX-LinkUp (Forwarding)     SX-LinkDown

Port Status: Enabled              Link Status: Up [1000Mbps-Full]

<Cmd>       <Description>
  h         Help for legends
  t         Toggle Port Status Enable/Disable
  a         Advanced Port Configuration
  g         Global Port Configuration
  q         Return to Previous Menu

Command>

Select module Next module Prev module Select port Next port Prev port
```

Figure 3-12 Port Configuration Menu for 1000BaseX ports

For a description of the current settings shown in the top portion of the screen, see “Current Port Settings” on page 3-22.

Enabling or Disabling a Port

Enabling or disabling a port is a manual operation. You can enable or disable a port to isolate network devices that may be causing problems on the network or to prevent unauthorized use of a port or station.

To enable or disable a port, use the following procedure.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. In the Basic Port Configuration Menu, use s, n, or p to select the port you want to enable or disable.
4. Type t to toggle the port's connection to either enabled or disabled status, as desired.

The port's status is changed immediately, and it is reflected in the Port Configuration Menu's Port Status indication and the Operating Status symbol for the port.

Advanced Port Configuration

The Advanced Port Configuration Menu allows you to control the port broadcast and multicast rate, to enable or disable 802.3x flow control, and to set the default priority of the port.

To access the Advanced Port Configuration Menu, from the Configuration Menu, type **p** to access the System Module Map, then select the module you want to configure. From the Port Configuration Menu, type a. The Advanced Port Configuration Menu appears for either 10/100BaseTX or 1000BaseX, as shown in Figure 3-13 and Figure 3-14.

Advanced 10/100BaseTX Port Configuration

```
IntraCore 8000 Advanced Port Config Menu   Module Type: (24-100TX)
Module: [1]                 Port:   [1]
                       1      8  9     16  17    24
                       ========  ========  ========
Operating Status:      +-------  --------  --------
Flow Ctrl:             *-------  --------  --------
Priority:              10001111  11111122  23333333

Max. Broadcast Rate:          N/A
Max. Multicast Rate:          N/A
802.3x Flow Control:          Enabled
Port Default Priority:        1

<Cmd>      <Description>
  h         Help for legends
  r         Set Max. Broadcast/Multicast Rate
  f         Toggle 802.3x Flow Control Enable/Disable
  i         Set Port Default Priority
  q         Return to Previous Menu

Command>

Select module Next module Prev module Select port Next port Prev port
```

Figure 3-13 Advanced Port Configuration Menu - 10/100BaseTX port

For a legend of the symbols used for the flow control and port priority table, type h and you will see the screen displayed in Figure 3-11.

Advanced 1000BaseX Port Configuration

```
IntraCore 8000 Basic Port Configuration Menu   Module Type: (2-GBIC)
Module: [1]
Port:   [1]            Port 1                      Port 2
                       ===========                 ===========
Flow Ctrl:             SX-LinkUp (Forwarding)      SX-LinkDown
Priority:              1                           1

Max. Broadcast Rate:          N/A
Max. Multicast Rate:          N/A
802.3x Flow Control:          Enabled
Port Default Priority:        1

<Cmd>      <Description>
  h         Help for legends
  r         Set Max. Broadcast/Multicast Rate
  f         Toggle 802.3x Flow Control Enable/Disable
  i         Set Port Default Priority
  q         Return to Previous Menu

Command>

Select module Next module Prev module Select port Next port Prev port
```

Figure 3-14 Advanced Port Configuration Menu - 1000BaseX port

The following subsections explain the configuration options in the Advanced Port Configuration Menu for 10/100BaseTX and 1000BaseX ports.

Current Settings

The settings shown in the top portion of the Advanced Port Configuration Menu are described in Table 3-8.

Setting	Description
Module Number	The number of the module of which the selected port is a member.
Module Type	Code for the type of module: 24-100TX, 2-GBIC, or 8-100FX. See Figure 3-9 for the full names of each module type.
Operating Status	This field displays status symbols for each of the current module's ports. For details, see the legend in Figure 3-11.
Flow Control	The status of flow control for the current port.When enabled, it allows you to control traffic and avoid congestion, such as when the port is receiving too much traffic for the available buffer resources.
Priority	The priority ranking for the port regarding data transmission during periods of peak or heavy on the traffic. Ports with higher priority take precedence when there is traffic congestion.
Max. Broadcast Rate	The maximum number of packets per second that can be broadcast by the current port to the network
Max. Multicast Rate	The maximum number of packets that can be multicast to all or selected ports on the network by the current port.

Table 3-8 Advanced Port Configuration Menu settings

Setting the Maximum Broadcast or Multicast Rate

Use the following procedure to set a limit on how many packets may be either broadcast or multicast from the current port.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. In the Basic Port Configuration Menu, type a to open the Advanced Port Configuration Menu.

4. Use s, n, or p to select the port for which you want to set the broadcast or multicast rate.
5. Type r to set the maximum broadcast or multicast rate for the selected port.
6. Enter the rate for broadcast or multicast and press Return.

The new maximum rate is displayed on the Advanced Port Configuration Menu.

Enabling or Disabling 802.3x Flow Control

Use the following procedure to control traffic and avoid congestion, such as when there is a shortage of buffer resources for the port. Flow control is accomplished by means of standard PAUSE control frames for each port, independent of all others. Before you can enable flow control for a port, that port must be configured to operate in Full Duplex mode.

If you enable flow control on a port, and that port runs short of buffer resources, the port will transmit PAUSE frames. When it receives them, the link partner obeys these PAUSE frames. When the low-resource situation is relieved, the port sends out PAUSE frames with zero time values. This ends the pause staste that was imposed on the end-station.

To enable flow control, first access the Port Configuration Menu by typing p in the Configuration Menu, then take the following steps.

1. Choose a module in the System Module Map.
2. In the Basic Port Configuration Menu, type a to open the Advanced Port Configuration Menu.
3. To select the port for which you want to enable or disable flow control, type s, n, or p.
4. To toggle flow control for the selected port, type f.

In the Advanced Port Configuration Menu, the Flow Control symbol for the selected port reflects its change in state, as does the 802.3x Flow Control setting.

▲ Important: When using this method of flow control, the link partner must be configured to recognize PAUSE frames.

Setting Port Default Priority

Use the following procedure to set the priority for a port. This priority setting determines the order in which the port forwards packets. Each port is associated with a traffic class: zero (0) is the lowest, and the default priority level. Seven (7) is the highest priority level.

1. Access the Port Configuration Menu by typing p in the Configuration Menu.
2. Choose a module in the System Module Map.
3. In the Basic Port Configuration Menu, type a to open the Advanced Port Configuration Menu.
4. Use s, n, or p to select the port for which you want to set the default priority.
5. Type i to set the priority for the selected port.
6. Enter the priority, from 0 to 7, and press Return.

The new default priority is shown on the Advanced Port Configuration Menu.

Global Port Configuration

The Global Port Configuration Menu allows you to simultaneously change the configuration information for all ports in a module.

To change the port configuration for all ports in a module, use the following procedure.

1. From the Configuration Menu, type p to access the Port Configuration Menu. A System Module Map appears, similar to Figure 3-9 on page 3-19.
2. Select the module that you want to configure globally. The Basic Port Configuration Menu appears, similar to Figure 3-10 on page 3-20.
   - *Note:* Your configuration choices will change the settings of all the ports in the module you select. The configuration of ports in other modules will be unaffected.
3. From the Basic Port Configuration Menu, type g. The Global Port Configuration Menu appears, for either

10/100BaseTX ports or 1000BaseX ports, as shown in Figure 3-15 and Figure 3-16.

```
IntraCore 8000 Global Port Configuration Menu  Module Type: (24-100TX)
Module: [1]
                        1      8 9      16  17    24
                        ========  ========  ========
Operating Status:       +-------  --------  --------
Auto Negotiation:       ********  ********  ********
Link Speed/Duplex:      Fhhhhhhh  hhhhhhhh  hhhhhhhh
Flow Ctrl:              *-------  --------  --------
Priority:               00001111  11111122  22333333


<Cmd>      <Description>
  h         Help for legends
  t         Select Global Ports Status Enable/Disable
  u         Select Global Auto-Negotiation/Manual
  l         Select Global 10M/100M bps Link Speed
  d         Select Global Half/Full Duplex
  o         Modify Global Auto-Negotiation Advertisement
  r         Set Global Max. Broadcast/Multicast Rate
  f         Toggle Global 802.3x Flow Control Enable/Disable
  i         Set Global Port Devault Priority
  q         Return to Previous Menu

Command>

Select module  Next module  Prev module
```

Figure 3-15 Global Port Configuration Menu - 10/100BaseTX ports

```
IntraCore 8000 Global Port Configuration Menu   Module Type: (2-GBIC)
Module: [1]
                        Port 1        Port 2
                        ===========   ===========
Operating Status:       SX-Enabled    SX-Enabled
Flow Ctrl:              Disabled       Disabled
Priority:               1              0

<Cmd>      <Description>
  h         Help for legends
  t         Select Global Port Status Enable/Disable
  r         Set Global Max. Broadcast/Multicast Rate
  f         Toggle Global 802.3x Flow Control Enable/Disable
  i         Set Global Port Default Priority
  q         Return to Previous Menu


Command>

Select module  Next module  Prev module
```

Figure 3-16 Global Port Configuration Menu - 1000BaseX ports

Follow the procedures in the "Port Configuration" and "Advanced Port Configuration" sections of this chapter.

Unicast Forwarding Database Configuration

The Unicast Forwarding Database Configuration Menu allows you to view and search for addresses in the IntraCore 8000's MAC Forwarding Table. It also provides options for displaying MAC addresses and IP/MAC binding by individual port or by VLAN.

The MAC Forwarding Table is a table of node addresses that the IntraCore 8000 automatically builds by "learning." It performs this task by monitoring the packets that pass through the IntraCore 8000, checking the source and destination addresses, and then recording the source address information in the table.

The IntraCore 8000 uses the information in this table to decide whether a frame should be forwarded to a particular destination port or "flooded" to all ports other than the received port. Each entry consists of three parts: the MAC address of the device, the port number on which it was received, and the VLAN number.

- *Note:* The MAC address table can hold a maximum of 8,192 entries.

When you type d in the Configuration Menu, the Unicast Forwarding Database Configuration Menu appears, as shown in Figure 3-17.

```
IntraCore 8000 Unicast Forwarding Database Configuration Menu

Age-out Time:           300 sec.
MAC Address Count:      33
IP Address Count:       21

<Cmd>      <Description>
  a         Display All Forwarding Database With/Without IP
  p         Display Forwarding Database By Port With/Without IP
  v         Display Forwarding Database by VLAN With/Without IP
  m         Search for MAC Address
  i         Search for IP Address
  t         Set Age-Out Time
  q         Return to Previous Menu


Command>
```

Figure 3-17 Unicast Forwarding Database Configuration Menu

Current Settings

Table 3-9 explains each setting on the Forwarding Database Configuration Menu.

Setting	Description
Age-out Time	The number of seconds that addresses are retained in the table. The default is 300 seconds. The range is from 10 to 1,000,000.
MAC Address Count	The number of entries currently in the MAC Address Table.
IP Address Count	The number of entries in the MAC Address Table that contain a corresponding IP address.

Table 3-9 Forwarding Database Configuration Menu settings

Displaying the Forwarding Database

Use the following procedure to view the Unicast Forwarding Database table.

1. Open the Unicast Forwarding Database Configuration Menu by typing d in the Configuration Menu.
2. Type either a, p, or v, depending on the range of MAC addresses you want to view.

   Type **a** to display the MAC addresses of all ports on the IntraCore 8000.

   Type p to specify a port, then see the MAC addresses for that port only.

   Type v to specify a VLAN, then see the MAC addresses for the member ports of that VLAN only.
3. At the prompt which appears, type y to see IP addresses in the display or type n to see the display without IP addresses, then press **Return**. The selected display appears.

Examples of the Unicast Forwarding Database table are shown in Figure 3-18 (all ports, without IP displayed) and Figure 3-19 (one port, without IP displayed).

- *Note:* When the IP addresses are displayed, the age and priority are not displayed, as shown in Figure 3-19.

The **Type** field refers to the type of MAC address. The Type setting may be:

- **S** —þstatic (set by management, and will *not* age out)
- **D** — dynamic (learned by the switch; will be aged out)
- **M** — multiple (associated with multiple IP addresses, as in the case of a router)
- I — Self (the IntraCore 8000's MAC address)

The **Pri** field refers to the priority setting for the port.

The **Age** field indicates the amount of time remaining before an entry ages out.

```
Entry Type : ( D = Dynamic , S = Static , I = Self )
+------+----+----+-----------------+---------+-----+----------+
|Module|Port|Type|   MAC Address   | VLAN ID | Pri |   Age    |
+------+----+----+-----------------+---------+-----+----------+
   1      6   D   00:00:94:75:2A:21    0001     0       252
   1      6   D   00:00:94:9A:BF:54    0001     0       300
   1      6   D   00:00:94:B4:66:48    0001     0       276
   1      6   D   00:00:94:B4:7A:8D    0001     0       292
   1      6   D   00:00:94:B5:1B:B1    0001     0       284
   -     --   I   00:00:94:DD:75:01    0001     0        --
   1      6   D   00:10:4B:36:91:AC    0001     0       300
   1      6   D   00:A0:24:9A:1E:4E    0001     0       284
   1      6   D   00:A0:CC:2C:57:29    0001     0       260
   1      6   D   00:E0:52:01:44:46    0001     0       300
   1      6   D   00:00:94:5D:E2:8D    0001     0       276
   1      6   D   00:00:94:10:E3:12    0001     0       246
   1      6   D   08:00:20:72:A0:1C    0001     0        81
   1      6   D   00:00:94:7B:02:C0    0001     0       291
   1      6   D   00:00:94:75:34:DE    0001     0         3
   1      6   D   00:00:94:75:31:DB    0001     0        21
   1      6   D   00:A0:CC:2C:60:CB    0001     0       144
   1      6   D   00:00:94:9A:2F:1C    0001     0       150
   1      6   D   00:00:94:75:2F:CF    0001     0       297
Press Next, Previous, or Quit
```

Figure 3-18 Unicast Forwarding Database, all ports, without IP displayed

In the forwarding database for all ports, the first screen shows the entries for devices connected to the first module's ports. If you scroll through the database, you can see the entries for each port of each module. For example, in
Figure 3-18, some MAC addresses for devices connected to port 6 of module 1 are shown.

```
Module: [1]  Port: [6]
Entry Type [T]: (D = Dynamic, S = Static, M = Multiple, I = Self)
+-+-+-+-----------------+---------------+
|M|P|T|   MAC Address   |       IP      |
+-+-+-+-----------------+---------------+
 1 6 D 00:00:94:10:80:1D  199.35.192.185
 1 6 D 00:E0:52:01:44:46  199.35.192.189
 1 6 D 00:00:94:A2:DE:56  199.35.192.181
 1 6 D 00:00:94:7A:CF:48  199.35.192.188
 1 6 D 00:00:94:92:F1:A8  199.35.192.182
 - - I 00:00:94:8E:F2:CC  199.35.192.187
 1 6 D 00:00:94:5D:E0:41  199.35.192.183
 1 6 D 00:00:94:5D:E1:9E  199.35.192.186
 1 6 D 08:00:20:80:5E:9C  199.35.192.184
 1 6 D 00:00:94:5D:E2:15  199.35.192.195
 1 6 D 00:00:94:5D:E2:8D  199.35.192.199
 1 6 D 00:00:94:10:E3:12  199.35.192.191
 1 6 D 08:00:20:72:A0:1C  199.35.192.198
 1 6 D 00:00:94:7B:02:C0  199.35.192.192
 1 6 D 00:00:94:75:34:DE  199.35.192.197
 1 6 D 00:00:94:75:31:DB  199.35.192.193
 1 6 D 00:A0:CC:2C:60:CB  199.35.192.196
 1 6 D 00:00:94:9A:2F:1C  199.35.192.194
 1 6 D 00:00:94:75:2F:CF  199.35.192.175
 Press Next, Previous, or Quit
```

Figure 3-19 Unicast Forwarding Database for a single port, with IP displayed

The Unicast Forwarding Database display for a single port shows only the entries for the devices connected to the selected port, as you can see in Figure 3-19.

Searching for a MAC Address

The Unicast Forwarding Database can be searched by MAC address or by IP address. To search for a specific MAC or IP address, use the following procedure.

1. Access the Unicast Forwarding Database Configuration Menu by typing d in the Configuration Menu.
2. Type m to search for a MAC address.

   Type i to search for an IP address.
3. Type the MAC or IP address at the prompt.
4. Press return.

If the address is located, it is displayed, with its associated information, as shown in Figure 3-20. If the address is not located, a message appears, stating this.

```
The MAC Address Search Summary
==============================
Module:          1
Port:            6
Type:            Dynamic
Age:             200
Priority:        0
MAC Address:     00:00:94:11:12:13
IP Address:      192.168.54.111


press any key to continue...
```

Figure 3-20 MAC Address Search summary

The Search Summary screen tells the location of the MAC or IP address, the module, port, and the Domain Name. Configuration information, such as the type, age, and priority are also displayed.

Setting the MAC Address Age-Out Time

This option sets the Age-Out Time for the MAC Forwarding Table.

The Age-Out Time is the number of seconds that addresses remain in the table after being learned by the IntraCore 8000. The default is 300 seconds.

Use the following procedure to set the MAC address Age-Out Time.

1. Access the Unicast Forwarding Database Configuration Menu by typing d in the Configuration Menu.
2. Type t to set the MAC Address Age-Out Time.
3. Enter the new Age-Out time (in seconds) at the prompt.
4. Press Return.

The MAC Address Age-Out Time is changed and is displayed at the top of the Unicast Forwarding Database Configuration Menu.

Image File Downloading Configuration

The Image File Downloading Configuration Menu allows you to upgrade your IntraCore 8000 system easily, using either TFTP or X/Y/Z modem protocol.

Type f in the Configuration Menu to see the Image File Downloading Configuration Menu, as shown in Figure 3-21.

```
IntraCore 8000  Image File Downloading Configuration Menu

<Cmd>           <Description>
  t              TFTP Image File Downloading Configuration
  x              X/Y/ZMODEM Image File Downloading Configuration
  q              Return to Previous Menu

Command>
```

Figure 3-21 Image File Downloading Configuration Menu

From the Image File Downloading Configuration Menu, select the downloading protocol. Type t to download the image file via TFTP or type x to download using the X/Y/Z modem protocol. The two subsections that follow describe downloading by each of the two protocols.

When Asanté issues a new version of software for the IntraCore 8000, you can obtain it from the Asanté World Wide Web site or by contacting Asanté Technical Support (see Appendix A, “Technical Support,” for details).

Image Downloading Through TFTP

To download a new image file in-band through TFTP, type t in the Image File Downloading Configuration Menu (option **g** in the Configuration Menu).
A screen similar to Figure 3-22 appears.

```
IntraCore 8000  TFTP File Downloading Menu

Bank 1 Image Version/Date       1.00T/May 07 1999 11:34:46
Bank 2 Image Version/Date       1.00U/Jul 29 1999 15:55:34 (Running)

File Type:            Image
Server IP:            192.168.52.211
File Name:            ic9k101.ima
Retry Count:          5
Destination Bank:     1

<Cmd>       <Description>
  s          Set Server IP Address
  f          Set File Name
  d          Download Image File to Destination Bank
  b          Download and Reboot from the Image File
  r          Set Retry count
  a          Toggle Destination Bank
  q          Return to Previous Menu

Command>
```

Figure 3-22 TFTP Image File Downloading Menu

Current Settings

Table 3-10 describes each setting on the TFTP Image Downloading Menu.

Setting	Description
Bank 1 Image Version/ Date	The version number and compilation date of runtime code that is stored in memory bank 1 on the IntraCore 8000.
Bank 2 Image Version/ Date	The version number and compilation date of runtime code that is stored in memory bank 2 on the IntraCore 8000. The (Running) designation indicates that the runtime code is currently running on this bank.
Server IP	IP address of network server containing software image file.
File Name	The software image file's name and network path.
Retry Count	Number of attempts the switch will make to download image file.
Destination Bank	Number of the memory bank where the image file will download.

Table 3-10 TFTP Image Download Menu settings

Performing a Software Upgrade at Runtime

The software image file must be downloaded from a server on your network that is running a TFTP server application.

▲ Important: Make sure the IntraCore 8000 is configured with an IP address. For details, see "Changing System IP Information" earlier in this chapter.

To upgrade the IntraCore 8000 software via TFTP, use the following procedure.

1. Access the TFTP Image File Downloading Configuration Menu by typing t in the Image File Downloading Configuration Menu.
2. Type s to set the image server IP address.
3. At the prompt, enter the IP address of the server containing the image file, then press Return.
4. Type f to set the image file name.
5. At the prompt, enter the image file's name and path, then press Return.
6. Type r to set the retry count.
7. At the prompt, enter the number of attempts the IntraCore 8000 will make to download the image file, then press Return.
8. Select the Destination Image Bank by using the a option. In a typical situation, you will want to select the Bank on which the software is not currently running, as shown in Figure 3-22.
9. To download the image file to the destination bank, type d. This option allows you to change the boot bank at a later time or to use the System Reset Configuration to schedule a reset, at which time the new software will be run.

   OR

   To download the image file and reset the switch, type b. This option immediately boots the IntraCore 8000 with the new version of software.

10 Type q to return to the Image File Downloading Menu.

Serial Downloading Configuration

The X/Y/Z Modem Image File Downloading Menu lets you download a new software image file for the IntraCore 8000 without interrupting the current operation.

To download a new image through the IntraCore 8000 management module's serial (console) port, type **x** in the Image File Downloading Configuration Menu. The X/Y/Z Modem Image File Downloading Menu appears, as shown in Figure 3-23.

```
IntraCore 8000  X/Y/ZMODEM Image File Downloading Menu

Bank 1 Image Version/Date      1.00T/May 07 1999 11:34:46
Bank 2 Image Version/Date      1.00U/Jul 29 1999 15:55:34 (Running)

Download Protocol:     ZMODEM
Current Baud Rate:     9600 bps
Destination Bank:      1

<Cmd>      <Description>
  x         Set download protocol to XMODEM
  y         Set download protocol to YMODEM
  z         Set download protocol to ZMODEM
  c         Change Baud Rate Setting
  d         Download Image File
  b         Download and Boot Image File
  a         Toggle Destination Bank
  q         Return to Previous Menu

Command>
```

Figure 3-23 X/Y/Z Modem Image File Downloading Menu

Current Settings

Table 3-11 describes the settings shown in the X/Y/Z Modem Image File Downloading Menu.

Setting	Description
Bank 1 Image Version/ Date	The version number and compilation date of runtime code that is stored in memory Bank 1 on the IntraCore 8000.
Bank 2 Image Version/ Date	The version number and compilation date of runtime code that is stored in memory Bank 2 on the IntraCore 8000.The (Running) designation indicates that the runtime code is currently running on this Bank.
Download Protocol	Current setting of the IntraCore 8000's serial download protocol.
Current Baud Rate	Transmission rate for the IntraCore 8000's serial port.
Destination Bank	Number of the memory bank where the image file will download.

Table 3-11 X/Y/Z Modem Image File Downloading settings

Performing a Software Upgrade

Use the following procedure to upgrade the IntraCore 8000 software through its serial (console) port.

1. In the Image File Download Configuration Menu, type x to open the X/Y/Z Modem Image File Downloading Menu.
2. Type x, y, or z to select the corresponding modem protocol.
   - *Note:* For information about these protocols, see the manual for your communications software.
3. Type c to select the console baud rate. The Baud Rate Setting Menu appears, as shown in Figure 3-24. The maximum baud rate currently supported is 57,600 bps.

```
Current Baud Rate:  9600 bps

Please select one from the following baud rate settings, or
press any other key to quit:

WARNING:   The user must use the same baud rate setting of the terminal
           after he/she confirms to change the baud rate setting of the
           console in order to work correctly.

<Cmd>      <Description>
  a         Set Baud Rate to 1200 bps
  b         Set Baud Rate to 2400 bps
  c         Set Baud Rate to 4800 bps
  d         Set Baud Rate to 9600 bps
  e         Set Baud Rate to 19200 bps
  f         Set Baud Rate to 38400 bps
  g         Set Baud Rate to 57600 bps

Choice>
```

Figure 3-24 Baud Rate Menu

4 Select one of the options in the above screen to select the required baud rate, and confirm it by typing y.

- *Note:* The baud rate default for console management is 9600 bps; in most cases the default will match the rate for the connected terminal. If you change the baud rate for the console port, the screen will display gartbled data unless the connected terminal is set to the same rate.

5 Type a to select the Destination Bank.

6 To download the image file, use any serial communications software such as Procomm Plus, HyperTerminal, ZTerm, etc. For file transfer instructions, follow the instruction manual of the serial communications software.

- *Note:* The terminal on which the serial communications software is running must have the same baud rate as the IntraCore 8000 management module console. The connection from the terminal to the switch console port must be an RS232C straight-through cable.

7 Type **d** to download to the selected destination bank or **b** to download and reset.

8 Type **q** to return to the previous menu after performing a successful download.

System Reset Configuration

The System Reset Configuration Menu allows you to reset the IntraCore 8000 by performing a "warm" reboot. It also allows you to schedule a reset up to 24 hours in advance.

To reset the IntraCore 8000, type r in the Configuration Menu. A screen similar to Figure 3-25 appears.

```
IntraCore 8000  System Reset Configuration Menu

Reset Status:          Stop
Reset Type:            Normal
Reset Countdown:       1 sec.

<Cmd>       <Description>
  s         Schedule Reset Time
  c         Cancel Reset
  r         Reset System
  d         Reset Switch to Factory Default
  i         Reset Switch to Factory Default except IP and Bootstrap
  q         Return to Previous Menu

Command>
```

Figure 3-25 System Reset Configuration Menu

Current Options

Table 3-12 describes the settings shown in the System Reset Configuration Menu.

Option	Description
Schedule Reset Time	Number of seconds until the scheduled reset.
Cancel Reset	Stops the scheduled reset.
Reset Switch	Performs a warm reboot to reset the IntraCore 8000 immediately.
Reset Switch to Factory Default	Resets the IntraCore 8000 to the original factory settings.
Reset Switch to Factory Default except IP & Bootstrap	Resets the IntraCore 8000 to the original factory settings without modifying the IP and Bootstrap configuration.

Table 3-12 System Reset Configuration options

Resetting the IntraCore 8000

To reset the IntraCore 8000, use the following procedure.

1. Open the System Reset Menu by typing r in the Configuration Menu.
2. Type r, **d** or **i**. Typing r resets the IntraCore 8000. Typing d resets the IntraCore 8000 to the factory default. Typing i resets the IntraCore 8000 to the factory default without affecting its IP and Bootstrap configuration.
3. Type y to confirm the reset or type n to cancel the reset.
   - *Note:* During the scheduled reset operation, you can see the reset countdown decrement by refreshing the screen.

Scheduling a System Reset

You can schedule the IntraCore 8000 to automatically perform a reset from one second up to 24 hours (86,400 seconds) in advance.

To schedule a reset, use the following procedure.

1. Open the System Reset Menu by typing r in the Configuration Menu.
2. Type s to schedule a reset time (within the specified range).
3. Enter the number of seconds the IntraCore 8000 will wait before it automatically resets.

   ▲ Important: The maximum number of seconds that can be entered is 86,400 (24 hours).

4. Press Return.

The IntraCore 8000 will reset automatically after the number of seconds you specified.

Viewing the System Log

The IntraCore 8000 system log records and displays any major system events on the switch, such as fatal errors, plugging in or removing a module, etc.

To view the system log, use the following procedure.

1. Type l in the Configuration Menu. The System Log Menu appears, as shown in Figure 3-26.

```
IntraCore 8000 System Log Menu

<Cmd>     <Description>
  l       Display System Log
  c       Clear System Log
  q       Return to previous menu




Command>
```

Figure 3-26 System Log Menu

2 Type d to display the current system log, as shown in Figure 3-27.

```
IntraCore 8000 System Log Summary
=================================================================
No.   D: H: M: S  Event
 1. 000:00:00:00  Reset NVDB sections to factory default
 2. 000:00:00:07  Spanning Tree Task Disabled
 3. 000:00:32:53  Spanning Tree Task Enabled
 4. 000:00:33:45  Spanning Tree Task Disabled
 5. 000:00:41:11  Spanning Tree Task Enabled
 6. 000:00:00:00  Reset NVDB section  0 to factory default
 7. 000:00:32:51  Spanning Tree Task Disabled
 8. 000:00:33:08  Spanning Tree Task Enabled
Quit  Next Page
```

Figure 3-27 System Log Summary

The system log displays any major system events that have occurred on the IntraCore 8000. If no major events have occurred, “System up” messages are displayed.

- *Note:* The system log holds a maximum of 64 entries.

3 Press any key to display the next page of System Log information.

Clearing the System Log

Use the following procedure to clear all entries from the current System Log.

1 Open the System Log Menu by typing l in the Configuration Menu.

2 Type c to clear the current System Log.

New entries will begin to accrue as events occur.

User Interface Configuration

The User Interface Configuration Menu lets you set the idle time-out periods for both the console and telnet user interfaces, change the password used for logging in to the Local Management Interface, and enable or disable the Web server.

To display the User Interface Configuration Menu, as shown in Figure 3-28, type u in the Configuration Menu.

```
IntraCore 8000 User Interface Configuration Menu

Console UI Idle Time Out          5 min
Telnet UI Idle Time Out           5 min

HTTP Server Status: ENABLED

Telnet Session Status:
Session      Status          Source IP
   1         Active          192.168.54.240
   2         Inactive        <none>
   3         Inactive        <none>
   4         Inactive        <none>

<Cmnd>          <Description>
  c              Set Console UI Time Out
  t              Set Telnet UI Time Out
  p              Change Administrator Password
  o              TOggle to Enable/Disable HTTP Server
  q              Return to previous menu

Command>
```

Figure 3-28 User Interface Configuration Menu

Current Settings

Table 3-13 describes the settings in the User Interface Configuration Menu.

Setting	Description
Console UI Idle Time-out	Duration of time the console will remain idle before returning to the Main Menu.
Telnet UI Idle Time-out	Duration of time the console will remain idle before closing the Telnet connection.

Setting	Description
HTTP Server Status	Enabled or Disabled.
Telnet Session Status	Inactive or Active, depending on whether session is in progress.
Telnet Session Source IP	The IP address of the device being used for telnet management.

Table 3-13 UI Time-out Settings

Setting Console Idle Time-out Period

Use the following procedure to set the console idle time-out.

1. Type c in the User Interface Configuration Menu.

   A prompt for the number of minutes is displayed.

2. Enter the desired idle time-out in minutes.

   - *Note:* The default time-out is 5 minutes. Range for time-out is 0-60 minutes (0 indicates no time-out).

   To exit without making any changes, press ctrl-c.

3. Press Return.

The new Console IU Idle Time Out is reflected in the User Interface Configuration Menu.

Setting Telnet Idle Time-out Period

Use the following procedure to change the Telnet Time-out.

1. Type t in the User Interface Configuration Menu.

   A prompt for the number of minutes is displayed.

2. Enter the desired idle time-out in minutes.

   - *Note:* The default time-out is 5 minutes. Range for time-out is 1-60. To exit without changes, press ctrl-c.

3. Press **Return**.

The new Telnet UI Idle Time Out is reflected in the User Interface Configuration Menu.

After you have configured the desired time-outs, type q to return to the previous menu.

Changing the Password

Use this option to change the password that the user must enter when they log in to the Local Management Interface or the Web server interface.

▲ Important: The factory default password is Asante. The password is case-sensitive.

To change the current Local Management Interface or Web-based Interface password, use the following procedure.

1. Type p in the User Interface Configuration Menu.
2. Type the password you have been using at the prompt.
3. Type a new password at the “Enter Current Password” prompt.

   ▲ Important: The password is case-sensitive. The password can be up to a maximum of 20 characters in length. The password characters can be any ASCII code.

4. Press Return.
5. Type the new password again at the confirmation password prompt.

   To cancel the change in password, type ctrl-c.

6. Press Return.

   The password change takes effect.

7. Type q to return to the Configuration Menu.

You will now need to enter the new password each time you log in to the Configuration Menu.

Enabling or Disabling the Web Server

The current HTTP Server Status is shown in the User Interface Configuration. For security, the web server is disabled by default.

Use the following procedure to toggle the status of the HTTP server:

- ❑ Type o in the User Interface Configuration Menu.

Viewing Statistics

Viewing statistics on a regular basis allows you to evaluate your network’s performance. You can view current statistics for the IntraCore 8000 on a per-port basis and can change your view of those statistics and the counters displayed in it.

To view statistics use the following procedure.

1 Type s in the Local Management Interface Main Menu. The System Module Map is displayed, as shown in Figure 3-29.

```
System Module Map
=================

Please select one of the following slots

 Slot     Description (Module Type)
 ----     -------------------------------
   1      24 10/100BaseTX ports Module (24-100TX)
   2      <none>
   3      1000BaseX ports Module (2-GBIC)
   4      <none>
   5      24 10/100BaseTX ports Module (24-100TX)
   6      <none>
   7      <none>
   8      <none>

Enter Module Number (1-8)>
```

Figure 3-29 Systems Module Map

2 Select the module for which you want to see statistics. The Port Statistics Counters screen is displayed, as shown in Figure 3-30.

```
IntraCore 8000 Port Statistics Counters           Module: 2  Port: 1

Elapsed Time Since Up:     000:00:00:55

<Counter Name>  <Total>  <Avg./s>  <Counter Name>    <Total>  <Avg./s>

Total RX Pkts     1474       26     Total RX Bytes   116246     2113
Dropped Pkts       185        3     Good Broadcast       57        1
Good Multicast       6        0     Undersize Pkts        0        0
Oversize Pkts        0        0     CRC/Align Errors      0        0
Fragments            0        0     FCS Errors            0        0
Collisions           0        0     Late Events           0        0
64-Byte Pkts       283        5     65-127 Pkts        1174       21
128-255 Pkts        12        0     256-511 Pkts          5        0
512-1023 Pkts        0        0     1024-1518 Pkts        0        0



<Cmd>  <Description>    <Cmd>  <Description>    <Cmd>  <Description>
   r     since reset      x     next module       n     next port
   t     stop refresh     v     prev module       p     prev port
   q     quit             g     select module     s     select port


Command>
```

Figure 3-30 Port Statistics Counters since system up

3 Use the s command to select a port for which you want to see the counters, or use n and p to find the port.

4 Use the g command to select a different module (group) in which you want to select a port, or use x and v to find the module.

5 Type t to stop the periodic updating of the counters, so you can record what they are at that time.

6 Type r to see a display of the same counters, but accrued since the last reset of the counters, as shown in Figure 3-31.

```
IntraCore 8000 Port Statistics Counters          Module: 2  Port: 1

Elapsed Time Since Reset:     000:00:00:55

<Counter Name>   <Total>  <Avg./s>  <Counter Name>   <Total>  <Avg./s>

Total RX Pkts       1474        26     Total RX Bytes   116246    2113
Dropped Pkts         185         3     Good Broadcast       57       1
Good Multicast         6         0     Undersize Pkts        0       0
Oversize Pkts          0         0     CRC/Align Errors      0       0
Fragments              0         0     FCS Errors            0       0
Collisions             0         0     Late Events           0       0
64-Byte Pkts         283         5     65-127 Pkts        1174      21
128-255 Pkts          12         0     256-511 Pkts          5       0
512-1023 Pkts          0         0     1024-1518 Pkts        0       0



<Cmd>  <Description>    <Cmd>  <Description>    <Cmd>  <Description>
   u    since system up   x     next module       n     next port
   t    stop refresh      v     prev module       p     prev port
   q    quit              g     select module     s     select port


Command>
```

Figure 3-31 Port Statistics Counters since reset

7 Type r to in the “since reset” screen reset the statistics counters so you can see them accrue again from zero.

8 Type q to quit either statistics screen and return to the Local Management Interface Main Menu.

For definitions of the counters, see Appendix B, “MIB Statistics.”

4
Advanced Management

This chapter describes advanced topics for management of the IntraCore 8000:

- ❑ Spanning Tree Protocol
- ❑ SNMP and RMON Management
- ❑ Security Management
- ❑ VLAN Management
- ❑ Multicast Management

Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a part of the IEEE 802.1D standard that provides for redundancy in a bridged LAN by allowing multiple links between points in the LAN.

Without the use of STP, multiple links in a bridged network will result in bridging loops, which allow excess broadcast traffic that can bring down an entire network.

Overview

The Spanning Tree Protocol reduces a network with multiple, redundant connections to one in which all points are connected (the protocol spans the network), but in which there is only one path between any two points (the paths are branched, as in a tree).

For example, in a large network with multiple paths, the same message will be broadcast over the network through multiple paths, resulting in a great amount of extra network traffic, and possibly, network downtime. This “closed path” or “bridged loop” among the networks can also start an unending packet-passing process.

▲ Important: To explain STP more effectively, the IntraCore 8000 is described as a bridge for this section of the manual.

How It Works

All bridges on the network communicate with each other using special packets called Bridge Protocol Data Units (BPDUs). The information exchanged in the BPDUs enables bridges on the network to:

- ❑ Elect a single bridge to be the root bridge.
- ❑ Calculate the shortest path from each bridge to the root.
- ❑ Select a designated bridge on each segment, which lies closest to the root and forwards traffic to the root.
- ❑ Select a port on each bridge to forward traffic to the root.
- ❑ Select the ports on each bridge that forward traffic, and place the redundant ports in blocking state.

Enabling and Disabling STP

The IntraCore 8000 is shipped with spanning tree enabled on all ports by default. To enable or disable STP on your IntraCore 8000, use the following procedure.

1. Type c to open the Configuration Menu.
2. Open the Spanning Tree Configuration Menu by typing s in the Configuration Menu. See Figure 4-1.
3. Type t to toggle STP to enabled or disabled.
4. If you select disabled, you are prompted to confirm the change.

   The STP status is changed. The status is displayed near the top of the Spanning Tree Configuration Menu.

Configuring Spanning Tree Parameters

To view the Spanning Tree Configuration Menu, as shown in Figure 4-1, type s in the Configuration Menu.

```
IntraCore 8000 Spanning Tree Configuration Menu

STP Status:         Enabled
Bridge ID:          8000 0000948EF37B

Designated Root:    0001 00503EA8B000
Root Port:          Module: 3  Port: 8
Root Path Cost:     110

Hello Time:         2 Sec.          Bridge Hello Time:          2 Sec.
Maximum Age:        20 Sec          Bridge Maximum Age:         20 Sec.
Forward Delay:      15 Sec.         Bridge Forward Delay:       15 Sec.

<Cmd>       <Description>
  t           Toggle STP Enable/Disable
  i           Set Bridge Priority
  h           Set Bridge Hello Time
  a           Set Bridge Maximum Age
  d           Set Bridge Forward Delay
  p           Spanning Tree Port Configuration
  q           Return to Previous Menu


Command>
```

Figure 4-1 Spanning Tree Configuration Menu

Spanning Tree Parameters

The operation of the spanning tree algorithm is governed by several parameters. You should attempt to set these parameters only if you have experience with the 802.1D specification.

Bridge Priority

Setting the Bridge Priority to a low value will make it more likely that the current bridge will become the root bridge. If the current bridge is located physically near the center of your network, you may wish to decrease the Bridge Priority from its default value of 0x8000. If the current bridge is near the edge of your network, it is best to leave the value of the Bridge Priority at its default.

Hello Time

This is the time period between BPDUs transmitted by each bridge.

Maximum Age

Each bridge should receive regular configuration BPDUs from the direction of the root bridge. If the maximum age timer expires before the bridge receives another BPDU, it assumes that a change in the topology has occurred, and it begins recalculating the spanning tree.

Forward Delay

After a recalculation of the spanning tree, the Forward Delay parameter regulates the delay before each port begins transmitting traffic. If a port begins forwarding traffic too soon, the network can be adversely affected. The permitted range of the Forward Delay is 4 to 30 seconds.

- *Note:* The Hello Time, Maximum Age, and Forward Delay are constrained by the following formula:

  ```
  (Hello Time + 1) <= Maximum Age <= 2 x (Forward Delay -1)
  ```

  In general, reducing the values of these timers will make the spanning tree react faster when the topology changes, but may cause temporary loops as the tree stabilizes in a new configuration. Lengthening the timers will make the tree react more slowly to changes in configuration but will make an unintended reconfiguration less likely. All of the bridges in the tree must agree on the values of these timers, so each bridge uses the ones advertised by the root.

Port Priority

If two ports are connected to the same segment, changing the Port Priority increases or decreases the probability that either port will be chosen for inclusion in the tree.

Current STP Settings

The following settings are displayed in the Spanning Tree Configuration Menu, as shown in Figure 4-1.

Setting	Description
STP Status	Whether spanning tree protocol is currently enabled or disabled.
Bridge ID	The Bridge Identifier of this bridge. The first part of the Bridge ID is the Bridge Priority. (If the Bridge ID is shown as 8000 000094EE5080, the 8000 is the Bridge Priority. The remainder is the MAC address of this bridge, which cannot be changed.).
Designated Root	The Bridge Identifier of the bridge that is currently the root bridge for the spanning tree.
Root Port	The port this bridge will use to forward traffic to the root. If this bridge is the root, the root port will be 0.
Root Path Cost	The cost as calculated by the spanning tree for messages to reach the root. If this bridge is the root, the cost will be 0.
Hello Time	The value of the timer currently being used by the bridge.
Maximum Age	The value of the maximum age timer currently being used.
Forward Delay	The value of the forward delay timer currently being used.
Bridge Hello Time	The value that will be used by the spanning tree if this bridge becomes the root bridge.
Bridge Maximum Age	The value that will be used by the spanning tree if this bridge becomes the root bridge.
Bridge Forward Delay	The value that will be used by the spanning tree if this bridge becomes the root bridge.

Table 4-1 Spanning Tree Configuration settings

Spanning Tree Port Configuration

To set the Port Priority and Port Path Cost values for STP, access the Spanning Tree Port Configuration Menu shown in Figure 4-2 by typing p in the Spanning Tree Configuration Menu.

```
IntraCore 8000 Spanning Tree Port Config. Menu  Module Type: (24-100TX)
Module: [1]
Port:   [1]

Port Speed:           100 Mbps
Port Status:          Enabled
Port State:           Forwarding
Port MAC Address:     00:00:93:8F:E3:7C
Port Priority:        0x80
Port Path Cost:       10

<Cmd>       <Description>
  i         Set Port Priority
  c         Set Port Path Cost
  q         Return to Previous Menu



Command>

Select module  Next module  Prev module  Select port  Next port  Prev port
```

Figure 4-2 Spanning Tree Port Configuration Menu

Setting Port Priority and Path Cost

The port priority is a bridge spanning tree parameter that ranks each port. When two or more ports have the same path cost, the STP selects the path with the highest priority (lowest numerical value). By changing the priority of a port, you can make it more or less likely to become the root port. The default value is 128, and the range is 0-255.

Port path cost is the bridge spanning tree parameter that assigns a cost factor to the port. The lower the assigned port path cost, the more likely the port is to be accessed. The default port path cost value is a result of the equation:

```
path cost = 1000/LAN speed (in Mbps)
```

Thus, for 10Mbps ports, the assigned default port path cost is 100. For 100Mbps ports, the default port path cost is 10. And for 1000Mbps ports, the assigned default port path cost is 1. The range is 1 to 65,535.

Use the following procedure to set the STP Port Priority and Path Cost values.

1. Access the Spanning Tree Port Configuration Menu by typing p in the Spanning Tree Configuration Menu.
2. Use the m, x, and v commands to select the module with the port you want to configure.
3. Use the s, n, and p commands to select the port you want to configure.
4. Type i to set the Port Priority.

   Type c to set the Port Path Cost.
5. Enter a value for the setting you are making.
6. Press Return.

The new Port Priority or Port Path Cost is displayed in the Spanning Tree Port Configuration Menu.

SNMP and RMON Management

The Simple Network Management Protocol (SNMP) may be used to manage the IntraCore 8000. The SNMP agent supports database objects that are defined in the following management information bases (MIBs):

- MIB II (RFC 1213)
- Bridge MIB (RFC 1493)
- RMON (RFC 1757) 4 groups - Ethernet Statistics, Ethernet History, Alarm, and Events (See next section for details)
- Private Asanté 9000 MIB

Any SNMP-based network management application can be used to manage the IntraCore 8000. For information on management of switches, refer to your SNMP software manual.

For details on console-based SNMP settings, see “SNMP Configuration” in Chapter 3.

RMON Management

Remote Network Monitoring (RMON) allows the network manager to gather data on the network's traffic for future retrieval. RMON is an Internet Standard defined in RFC1757.

Using RMON, a network monitor (also called a probe) listens to traffic on the network and gathers statistics that may be retrieved later by a network management station using SNMP, as described in the previous section.

The four groups of RMON that are supported by the IntraCore 8000 are described in the following sub-sections.

The IntraCore 8000 switches provide control of the RMON groups only through SNMP. For information on controlling RMON groups, please refer to the documentation for your SNMP management application.

For more information about RMON, please see RFC1757, "Remote Network Monitoring Management Information Base," available from the FTP site listed in Appendix A.

Ethernet Statistics Group

The Ethernet statistics group contains statistics measured on each port of the IntraCore 8000. These are cumulative counters that start at zero each time the IntraCore 8000 is reset. The Statistics Group is automatically implemented by the IntraCore 8000.

Ethernet History Group

The Ethernet history group records periodic statistical samples from ports on the IntraCore 8000 and stores them for later retrieval. A network manager can use the data to analyze how network traffic has varied over a period of time.

Alarm Group

The alarm group takes periodic statistical samples from variables in the IntraCore 8000 and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.

Event Group

The event group controls the generation and notification of events from the IntraCore 8000. The alarm and event groups together allow the network manager to configure RMON so that if a particular statistic (such as the number of bad frames) goes higher than a certain level, the IntraCore 8000 will send a trap to its configured trap receivers, notifying the manager of the

event. For information on configuring trap receivers, see “SNMP Configuration” in Chapter 3.

Security Management

The IntraCore 8000’s security management options are summarized in Table 4-2.

Security Option	Description	Action
Duplicated IP Detection (Monitoring)	Detects the use of a single IP address by two stations.	Detects and logs MAC addresses of both stations and the ports they accessed.
Duplicated IP Trap		Sends trap with MAC addresses of both stations and the ports they accessed.
Station Movement Trap	Detects the movement of any end station from one port to another.	Sends trap with the station’s MAC address and IP address (if available) and the switch’s port numbers.
Port New Node Trap	Detects the connection of any new device to the secured port.	Sends trap with the new node’s MAC address and IP address (if available) and the port to which they are connected.
Port Trusted MAC Address	Creates a set of port-trusted MAC addresses for use by other security measures.	None.
Port Intruder Detection Trap	Disallows traffic from MAC addresses not belonging to the port trusted MAC address set. Station movement is also disallowed.	Sends trap with intruder’s MAC address.
Port Lock	Disallows traffic from MAC addresses that do not belong to the port trusted MAC address set. Station movement is also disallowed.	Disables the port if an intruder is detected. Sends trap with the port number, and the intruder’s MAC address, VLAN ID, and IP address (if available).

Table 4-2 Security Management Options

To access the Security Management Menu, type t in the Configuration Menu.
A screen similar to Figure 4-3 appears.

```
IntraCore 8000 Security Management Menu

Duplicated-IP Monitoring Status: Enable
Duplicated-IP Trap Status:       Enable
Station Movement Trap Status:    Disable

<Cmd>     <Description>
  p       Port Security Configuration
  d       Toggle Duplicated-IP Detection Enable/Disable
  i       Toggle Duplicated-IP Trap Enable/Disable
  l       Display Duplicated-IP List
  s       Toggle Station Movement Trap Enable/Disable
  r       Reset All Security Configuration to Factory Default
  q       Return to previous menu

Command> p
```

Figure 4-3 Security Management Menu

Current Settings

The following settings are displayed in the Security Management Menu screen.

Setting	Description
Duplicated IP Monitoring Status	Whether duplicated IP monitoring (detection) is currently enabled or disabled.
Duplicated IP Trap Status	Whether duplicated IP trap is currently enabled or disabled.
Station Movement Trap Status	Whether station movement trap is currently enabled or disabled.

Table 4-3 Security Traps

▲ Important! For any traps (alerts) to be sent, you must designate one or more devices as trap receivers. See “SNMP Configuration” in Chapter 3.

Duplicated IP Detection and Trap

The duplicated IP detection and duplicated IP trap security measures allow you to monitor the use of a single IP address by two stations.

If you enable duplicated IP detection, the switch starts monitoring the broadcast Address Resolution Protocol (ARP) traffic from all of its ports, to detect duplicated IP address conditions. When duplicate IPs are used on the system, the MAC addresses of both stations and the ports they accessed are logged.

If you enable both duplicated IP detection and duplicated IP trap, the designated trap receiver gets an alert each time a duplicated IP address is used on the system. In order to send duplicated IP traps, duplicated IP detection must be enabled.

By default, duplicated IP detection and trapping are enabled.

Enabling and Disabling Duplicated IP Detection

To enable or disable detection of duplicated IP addresses:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type d to toggle duplicated IP detection.

Enabling and Disabling Duplicated IP Trap

To enable the sending of a trap when a duplicated IP is detected, you must first enable duplicated IP detection. See the previous subsection, “Enabling and Disabling Duplicated IP Detection.”

To enable or disable the sending of a trap when a duplicated IP is detected:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type i to toggle duplicated IP trap.

Viewing a List of Duplicated IP Addresses

To view a list of duplicated IP addresses that have been detected at the IntraCore 8000:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type l to display the duplicated IP list. A screen appears,

similar to Figure 4-4.

```
Duplicated-IP List
+--------------+-----------------+-+-+-----------------+-+-+
|   IP Address  |     Owner MAC    |M|P|    Spoofer MAC    |M|P|
+--------------+-----------------+-+-+-----------------+-+-+
 192.203.54.222  00:00:94:00:00:01  1 1  00:00:94:00:00:02  1 2
 192.203.54.223  00:00:94:00:00:04  1 3  00:00:94:00:00:02  1 2
 192.203.54.224  00:00:94:00:00:05  1 4  00:00:94:00:00:02  1 2
 
 
 
 
 
 
 
Press <q> to Quit, or, press any key to continue...
```

Figure 4-4 Duplicated IP address list

Enabling and Disabling Station Movement Trap

The station movement trap security measure ensures that when any end station is moved from one switch port to another, an alert is sent to the designated trap receiver. Station movement is detected when a station's MAC address (already learned by the switch) appears on a different switch port. The station movement trap includes the station's MAC address and IP address (if available) and the switch's port numbers.

By default, station movement trap is disabled.

To enable or disable detection of the movement of a station on the IntraCore 8000:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type s to toggle station movement trap.

Configuring Port Security

To access the Port Security Configuration Menu, type t in the Configuration Menu to access the Security Management Menu, then type p to access the Port Security Configuration Menu. A screen similar to Figure 4-5 appears.

```
IntraCore 8000 Port Security Configuration Menu Module Type: [24-100TX/RJ45]
Module: 01 Port: 01

Module Port Security Info:
[+: Port Security Enabled, -: No Port Security, !: Port Disabled By Security]
Port Security Status:  [01]-------- [09]-------- [17]-------- [25]XXXXXXXX

Port Security Type:  [<none>]
Port New Node Detect Trap Status:  [<none>]
Port Intruder Detect Trap Status:  [<none>]
Port Trusted MAC Address:  [<none>]

<Cmd>     <Description>
  u       Set\Clear Port Security
  t       Toggle Port Security Trap Enable/Disable
  i       Insert/Modify Port Trusted MAC Address
  d       Display Port Intruder Nodes
  h       Port Security Help
  q       Return to previous menu


Command>
Select Module Next module Prev module Select port Next port Prev port
```

Figure 4-5 Port Security Configuration Menu

Current Settings

The following settings are displayed in the Port Security Configuration Menu screen.

Setting	Description
Port Security Status	Status of security for each port: enabled, disabled by setting, or disabled in response to a security intrusion.

Setting	Description
Port Security Type	Level of port security enabled. There are three levels of security: • New node detection trap (security level 1) • Trusted MAC address forwarding with port lock (security level 2) • Trusted MAC address forwarding with intruder lock (security level 3)
Port New Node Detect Trap Status	Whether port new node detect trap is currently enabled or disabled.
Port Intruder Detect Trap Status	Whether port intruder detect trap is currently enabled or disabled.
Port Trusted MAC Address	MAC address currently specified as the port trusted MAC.

Table 4-4 Port Security Configuration Settings

Configuring Port New Node Detection Trap

The port new node detection trap security measure (also called "port security trap") ensures that when any new device is connected to the secured port, an alert will be sent to the designated trap receiver. The new device is detected when it is connected to the IntraCore 8000 and its MAC address is recognized as one not present in the current address table. The information shown in the alert is the new node's MAC address and IP address (if available) and the port to which they are connected.

Once a device has been connected and has generated traffic on the network, the trap will not be re-sent. If the switch ages out the MAC address of a connected device from its forwarding database, new traffic from that device will result in a new node trap being sent. The default age-out time is 300 seconds. You may reduce the number of traps sent by lengthening the age-out time, as explained in "Setting the MAC Address Age-Out Time" in Chapter 3.

By default, New Node detection is disabled.

To enable or disable detection of a new node on the system, you must first set the security level on a port or group of ports to **1**. Then, if it is not already enabled, you must enable New Node detection.

To set security level 1 on a port:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type p to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Select **u** to Set/Clear port security.
4. Type **s** to set security.
5. Type the numbers of the ports for which you want to set the security. You can specify a single port, a series of port numbers separated by commas, a range of ports shown with a hyphen, or a combination of ranges and single ports. For example, you can type **1-8, 14** to specify ports one through eight, and port fourteen. See help for more information.
6. Type **1** for Port Security Level 1.

To enable New Node detection:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type p to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Type t to choose Toggle Port Security Trap.
4. Type **1** to toggle the new node trap (if it is not already enabled).

Configuring Port Lock and Intruder Lock

The port intruder security measure allows you to create a port-trusted MAC address which is allowed to direct traffic to the port. Attempts to send traffic to the port from other stations are regarded as security intrusions, and can be disallowed. The security measure may be enabled as a port lock (security level 2) or an intruder lock (security level 3).

- *Note:* The three security levels are mutually exclusive; a port can have either security level1, level2, or level 3, but never a combination of security levels.

To configure security level 2 or 3, you must specify the port-trusted MAC address. You can either specify the address directly, or direct the system to trust the address of the first station that addresses the port. By trusting the first station to address the port, you can configure port security before you know which system will ultimately use that port.

When security level 2 (port lock) is enabled and an intruder attempts to direct traffic to the port, the port is immediately disabled. The port is then re-enabled only by clearing the security level by management.

When security level 3 (intruder lock) is enabled and an intruder attempts to direct traffic to the port, the switch locks out the intruder's MAC address; it will not accept any traffic from that station. The intruder's address is then re-enabled only by clearing the security level by management.

▲ **Important:** If you set security level 2 or 3, you should also set the Intruder Trap. If you do not set this trap, you will not receive notification that the port has been disabled. See "Setting the Intruder Trap."

By default, security levels 2 and 3 are both disabled.

Configuring Security Level 2 or Level 3

To set security level 2 (port lock) or level 3 (intruder lock) on a port:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type p to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Use the commands at the bottom of the menu to navigate to the port you want to want to configure.
4. Select **u** to Set/Clear port security.
5. Type **s** to set security.
6. Type **2** to select Port Security with Port Lock, or **3** to select Port Security with Intruder Lock.
7. Type **1** to have the system trust the first station that addresses this port, or type **2** to enter a specific port-

trusted MAC address. If you type **2**, you will be prompted to enter the address as follows: **xx:xx:xx:xx:xx:xx** where the values are hexadecimal, separated by colons.

Setting the Intruder Trap

If you set security level 2 or 3, you should also ensure the Intruder Trap is set. Enabling this trap directs the system to send an alert to the designated trap receiver when an intruder tries to access the port.

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type p to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Type t to choose Toggle Port Security Trap.
4. Type **2** to toggle the new node trap (if it is not already enabled).

Inserting/Modifying a Port Trusted MAC Address

When you set port security level 2 or 3 for a port, you specify the port-trusted MAC address. You can change that address for a port without completing all the steps to set the port security.

To add or change the port-trusted MAC address:

1. From the Configuration Menu, type t to access the Security Management Menu.
2. Type p to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Type i, then follow the instructions on the screen.

Resetting Security to Defaults

To reset the security measures on the IntraCore 8000 to the factory defaults, access the Security Management Menu by typing t in the Configuration Menu. Then type r to reset all of the security configurations that have been changed back to the factory-set defaults. These defaults and their meanings are discussed in the sections on each security measure, earlier in this chapter.

VLAN Management

A *virtual* LAN, or VLAN, is a logical grouping that allows stations to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of a network.

The IntraCore 8000 supports port-based VLANs, in compliance with the IEEE 802.1Q standard. The following subsections describe the concepts and details needed to configure and manage VLANs on IntraCore switches.

VLAN Specifications for the IntraCore 8000

The IntraCore 8000 supports the following features of the IEEE 802.1Q standard:

- ❑ Port-based VLAN management
- ❑ Up to 64 manually-configurable VLANs
- ❑ Default VLAN
- ❑ VLAN creation and deletion
- ❑ VLAN port member addition and deletion
- ❑ VLAN untagged set addition and deletion
- ❑ Configurable VID range: 2 to 4094
- ❑ Port VID configurable range: 1 to 4094
- ❑ Port ingress filtering
- ❑ Port admit frame type
- ❑ Independent VLAN learning (IVL)
- ❑ Shared VLAN learning (SVL)
- ❑ GVRP for dynamic VLAN learning (to be supported; later versions)
- ❑ Single STP (Spanning Tree Protocol) spanning multiple VLANs
- ❑ SNMP-based VLAN management

Other VLAN Features in IntraCore 8000

- ❑ VLAN management security
- ❑ VLAN MAC address insertion and removal
- ❑ Console UI management of VLANs
- ❑ Web interface management of VLANs

The management operations allowed are:

- ❑ Creation
- ❑ Deletion
- ❑ Name configuration
- ❑ VID change configuration
- ❑ Adding and deleting port members
- ❑ Adding and deleting untagged sets
- ❑ Sharing and unsharing VLANs
- ❑ Inserting and removing MAC addresses
- ❑ Toggling management access

Overview of VLANs

This section describes the concepts needed to configure and manage VLANs on IntraCore switches.

Benefits of VLAN Management

Unnecessary flooded traffic wastes bandwidth on a LAN, potentially clogging the network. Flooded traffic is traffic that is sent to all ports on the switch because the destination is a broadcast or multicast address, or because the location of the destination is unknown.

Traditional layer 2 bridges and switches attempt to limit unnecessary flooded traffic by learning the addresses of stations on the switch. But as traffic expands rapidly on today's networks, bandwidth wastage from layer 2 flooding can easily become a network bottleneck.

The traditional solution to the problem of broadcast flooding is to use a layer 3 device like a router. The trade-offs that accompany the use of routers include higher initial cost, more latency with decreased network performance, and higher maintenance and configuration expenses.

A VLAN localizes flooded traffic to parts of LAN segments rather than to a whole LAN. VLANs offer a simple and efficient solution that enhances network performance, bandwidth utilization, and network security by localizing flooded traffic.

Port-based VLANs are the simplest of many VLAN approaches that solve the problem of unnecessary flooding. A port-based VLAN allows the administrator to assign individual ports on a switch to a VLAN. Any broadcast, multicast, or unknown unicast traffic received on a port in a VLAN is flooded only to the other ports in the VLAN rather than to all ports in the system. This greatly reduces unnecessary traffic in a network.

For the most complete information about configuring VLANs in an 802.1Q environment, see the standard, available from IEEE <http://www.ieee.org>.

Tagged and Untagged Frames

In a network with only one switch, the switch itself can keep track of which ports belong to which VLANs.

In a network with multiple switches, information about which VLAN an ethernet frame belongs to must be sent along with the frame. This is done by inserting a tag field in the frame, as defined in IEEE 802.1Q. The tag includes the VID to identify the frame's VLAN. When a port receives a tagged frame, it can then pass the frame to other port members of the same VLAN.

When you add a port to a VLAN, you can specify whether or not frames originating from that port will be tagged. If the port is configured to send tagged frames, then its traffic will be associated with the VLAN identified in the tags.

If it receives an untagged frame, a port has no way to determine the originating VLAN. In that case, the port can be configured to send the frame as is, to aribtrarily assign a specific tag to the frame, or to drop the frame.

Abbreviations

The following abbreviations are used throughout this section.

FID	Filtering ID
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
ISL	Inter-Switch Link
MGMT	Management

PVID	A tagged port's VLAN ID (range is 1 to 4094)
STP	Spanning Tree Protocol
Tagged Frame	Frame with 802.1Q VLAN tag header
Untagged Frame	Frame either without a tag header, or with this header and with VID = 0
VID	VLAN ID (range is 1 to 4095)

VLAN Groups

A VLAN group is the sum total of ports on a switch that are assigned to a specific VLAN. IntraCore 8000 supports 64 manually-configurable VLANs on the network. Each switch maintains its own list of VLAN indexes between 1 and 64. Each VLAN is uniquely identified by a 12-bit (1-4095) VLAN ID (VID).

VID = 1 is reserved for the default VLAN, and VID 4095 is reserved to accomodate egress filtering. No two VLANs can have the same VID or VLAN index if they reside on the same switch.

Two VLANs can have the same VID and VLAN index if they reside on different switches. To connect VLANs or VLAN groups on different switches, you must configure a port as an Inter-switch Link (ISL). (See "Configuring Inter-Switch Links.")

Default VLAN

The IntraCore 8000 is configured by default with a single VLAN, with VID = 1; by default, all ports on the switch are assigned to VLAN 1. By default, the ports are also in the VLAN's untagged set, which means they send only untagged frames. The effect is that by default, a port is not limited by any VLAN boundaries, and strips VLAN data from all frames on egress.

Port VLAN ID

Each port has a Port VLAN ID (PVID), which is used to determine where to send untagged frames. If the port receives an untagged frame, it passes the frame to the VLAN identified by the PVID. By default, a port has PVID = 1, which is the same as the default VID.

If you specify that a port receives untagged and tagged frames, and also provide a PVID, the port will send all untagged frames to that VLAN. If you specify that a port drops all untagged frames, that specification sets the PVID to 4095.

VLAN Port Membership and Untagging

Port members can be added to and deleted from a VLAN Group via the VLAN Management Menu (see “Configuring Static VLAN Groups”). When you add it to a VLAN, you configure a port to determine its participation in the VLAN.

The VLAN Untagged Set. When you add a port member to a VLAN, it is added to the untagged set by default. This means the frames sent out on this port will be untagged. If you want the port to send tagged frames, you must delete the port from the VLAN’s untagged set (see “Specifying Tagging or No Tagging for a Port”).

No port can transmit both tagged and untagged frames on the same VLAN. However, it is possible for a port to be a member of more than one VLAN, and to transmit tagged frames for one VLAN and untagged frames for the other.

PVID - Egress Filtering. For a port that receives untagged frames, you can assign a Port VLAN ID (PVID). This determines that the port will send all untagged frames to the VLAN whose VID matches the PVID (see “Configuring VLAN Port Attributes”).

Receive Frame Type. You can specify whether a port receives all frames, or only tagged frames. If a port is configured to receive only tagged frames, any untagged frames received by the port are dropped. In this case, the PVID has not meaning, and it is set to 4095. Receiveing only tagged frames is especially important for setting up inter-switch links. (For more information, see “Configuring Port Receive Frame Type.”)

Ingress Filtering. In addition to Receive Frame Type, you can can also specify that the port only accepts and passes on frames that are tagged with a VID of a VLAN to which the port is a member. For example, if the port is a member of VLAN 1, it will only accept tagged frames with VID 1 in the tag. (For more information, see “Enabling and Disabling Port Ingress Filtering.”.)

Independent vs. Shared Learning

One problem addressed by a VLAN is the routing of traffic to unknown destination MAC addresses. Each VLAN maintains a table of learned addresses, similar to the way traditional layer 2 bridges learn the addresses of unknown destinations. Address learning for a VLAN can be independent or shared; shared learning means that all VLANS on a switch share a single address table. (See “Specifying Shared or Independent Address Learning.”)

By default, independent learning of addresses is enabled. Under independent learning, all addresses learned in a VLAN are stored in an address table for that VLAN only, and all forwarding decisions for that VLAN are made by consulting that table. This can sometimes cause unexpected results if a port is a member of more than one VLAN.

For example, assume a port is a member of VID 1 and VID 2, and VID 1 has already learned MAC address X. Unicast traffic from the port that is destined for X will be forwarded correctly in VLAN 1. But if the address is not present in the VLAN 2 forwarding table, the frame will be flooded to all ports in VLAN 2.

To prevent this undesired flooding, the address tables may be shared. When shared learning is enabled, a single forwarding table is used by all VLANs that are members of the shared group.

Each address database in the system is represented by a Filtering ID (FID). For independent learning VLANs, the FIDs are assigned by the system beginning from 0. Shared learning VLANs are represented by FIDs beginning at 65.

Inter-Switch Links

An inter-switch link (ISL) is a port that connects VLANS that reside on two different switches; it's the means to share VLAN information between switches on a network.

For example, consider the two-switch network in Figure 4-6, which connects the ethernet segments, E-1 through E-9. Assume port 1 on each switch is set up as default; it passes untagged frames. Also assume port 2 on each switch is configured to only accept tagged frames, which limits traffic to VLAN 1. In that case, VID 1 frames from E-1 will never reach E-5.

An ISL is necessary to connect VLAN 1 across the switches. This is done by configuring port 1 as a member of VLAN 1 on both switch 1 and switch 2. Both instances of port 1 must transmit tagged frames, and a typical ISL is also configured to drop untagged frames. In that case, VLAN 1 is connected across the switches.

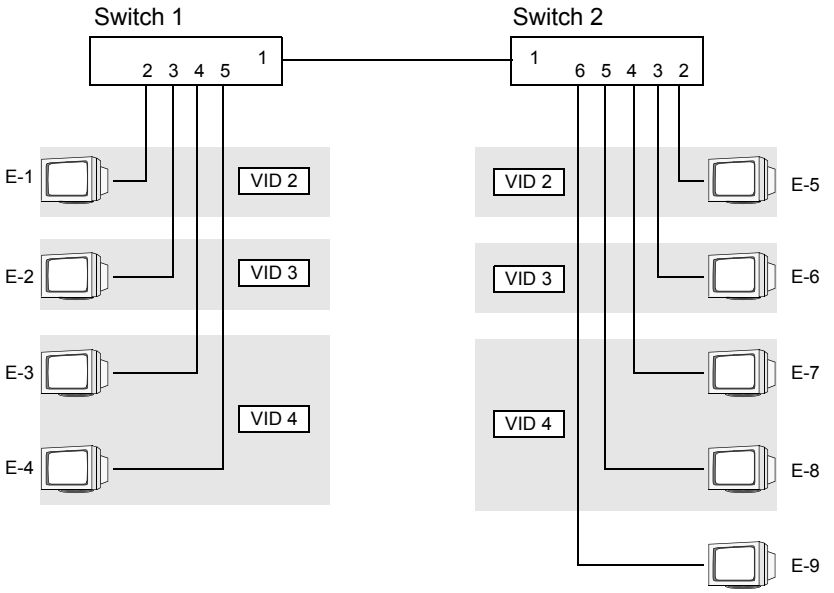


Figure 4-6 An Inter-Switch Link

The configuration of the ISL ports and the other ports on each switch will determine how tagged frames are transmitted across the switches. For example, if you require frames from VLANs 2 and 3 to cross the switches, the ports should have the following configuration for both switches:

Port	Receive Frame Type	Ingress Filter	VLANs	Untagset	PVID
1	802.1Q - Only	Disabled	V2, V3	No	4095
2	All Frames	Disabled	V2	No	V2
3	All Frames	Disabled	V3	No	V3
4	All Frames	Disabled	V4	No	V4
5	All Frames	Disabled	V4	No	V4
6 (Sw 2)	All Frames	Disabled	V1 (Default)	Yes	V1

In this case, VLAN 2 and VLAN 3 are linked across the switch. However, VLAN 4 is not; for example, frames from E-3 and E-4 cannot reach E-7 and

E-8. And because port 1 only accepts tagged frames, any untagged frames from E-9 will not cross from switch 2 to switch 1.

If you want VLAN 2 to pass frames to and from E-9, you need to configure the ISL differently. For example, you could change port 1 on both switches as follows:

Port	Receive Frame Type	Ingress Filter	VLANs	Untagset	PVID
1	All Frames	Disabled	V3	No	V2
			V2	Yes	

In this case, if port 1 receives an untagged frame, it assigns the frame to VLAN 2; for example, VLAN 2 will be flooded with frames from E-9.

On the other hand, when port 1 transmits a frame from VLAN 2, it removes the tag. Since all the other ports accept untagged frames, those frames will flood VLAN 3 on both switches, and VLAN 4 on the originating switch.

To see the menus and steps to configure an ISL, see “Configuring Inter-Switch Links.”

Configuring VLAN Management

To access the VLAN Management Menu, type v in the Configuration Menu. A screen similar to Figure 4-7 appears.

```
IntraCore 8000 VLAN Management Menu

VLAN Version:                   1    VLAN Type:           Port Based
Max. Supported VLAN ID:      4094    Max. Supported VLANs:    64
Number of VLANs Configured:     1    Number of Active VLANs:  1


<Cmd>     <Description>
  g       GVRP Configuration
  s       VLAN Group Static Configuration
  p       VLAN Port Attribute Configuration
  d       Display VLAN Groups Summary
  m       Display Module Port VLAN Summary
  f       VLAN FID-VID Association Summary
  r       Reset VLAN Configuration to factory default
  q       Return to previous menu




Command>
```

Figure 4-7 VLAN Management Menu

Current Settings

Table 4-5 describes each setting on the VLAN Management Menu.

Setting	Description
VLAN Version	IEEE 802.1Q version number.
VLAN Type	Port-based or SNMP-based.
Max. Supported VLAN ID	The IntraCore 8000 supports 4094 VLAN IDs.
Max. Supported VLANs	The IntraCore 8000 supports 64 VLANs.
Number of VLANs Configured	Number of VLANs currently present on the switch.
Number of Active VLANs	Number of VLANs currently active on the switch.

Table 4-5 VLAN Management Settings

Configuring Static VLAN Groups

To access the VLAN Group Static Configuration Menu, type v in the Configuration Menu to access the VLAN Management Menu, then type s to access the VLAN Group Static Configuration Menu. A screen similar to Figure 4-8 appears.

```
IntraCore 8000 VLAN Group Static Configuration Menu   VLAN Index: [01]
Module   Port List  1      8  9     16  17    24  25    32
======              ========  ========  ========  ========
  1  +: static      ++++++++  ++++++++  ++++++++  XXXXXXXX
  2  d: dynamic     ++++++++  ++++++++  ++++++++  XXXXXXXX
  3  -: Not Member  ++XXXXXX  XXXXXXXX  XXXXXXXX  XXXXXXXX
  4
  5
  6
  7
  8

VID: 0001    Created By: Mgmt      Name: Default VLAN
FID: 0000    Mgm Access: Enable    Status: Active, Independent

<Cmd>     <Description>           <Cmd>     <Description>
  c       Create VLAN               r       Remove VLAN
  e       Set VLAN Name             t       Toggle Mgmt Access
  a       Add Port Members          d       Delete Port Members
  m       Move ports to this VLAN


Command>
Select VLAN   Next VLAN   Prev VLAN   Advanced Config   Help   Quit
```

Figure 4-8 VLAN Group Static Configuration Menu

Navigate to the VLAN that you want to configure by typing a command as shown at the bottom of the screen. With the Select command, you select a VLAN by its index; you can type the index of an existing VLAN, or the index of a VLAN you will create.

Current Settings

Table 4-6 describes each setting on the VLAN Group Static Configuration Menu screen.

Setting	Description
VLAN Index	The VLAN Index of the VLAN group for which the information on the screen applies. The index is maintained by the system, and is not necessarily the same as the VID.
Port List	Shows each port's current membership status for this VLAN group.
VID	VLAN ID.
FID	Filtering ID.
Created By	Creator of this VLAN group; either Mgmt or GVRP.
Mgm Access	Whether management access is currently enabled or disabled.
Name	The name arbitrarily assigned to the VLAN group.
Status	Whether the VLAN group is active or inactive, and whether independent learning or shared learning of addresses is enabled.

Table 4-6 VLAN Group Static Configuration Settings

Creating a VLAN

To create a VLAN, you must first find a free VLAN index. From the VLAN Group Static Configuration Menu, type **d**. This displays a list of all the VLAN indexes and VID's that are currently in use. Decide on the index and VID you want to use for the new VLAN.

To create the VLAN:

1. Type **s** to select a VLAN, and then enter the VLAN index you decided to use. You will notice that the VID for an unused VLAN is 0000.
2. Type **c** to create the new VLAN and enter the VID you decided to use.
3. Enter a name for the VLAN.

4 Enter the modules and ports to assign to the VLAN. You specify module and port separated by a colon. For example, **1:8** assigns port 8 to module 1. You can make more than one assignment, separated by commas; **1:8, 2:8** assigns port 8 to modules 1 and 2. You can also assign ranges and lists of ports to a module; **1:1-3, 8, 2:4-7** assigns ports 1, 2, 3, and 8 to module 1, and ports 4, 5, 6, and 7 to module 2. See Help for more information about specifying modules and ports.

Removing a VLAN

To remove the VLAN, from the VLAN Group Static Configuration Menu, type **s** to select the VLAN, then type **r** to remove it.

Naming a VLAN

To name the VLAN, from the VLAN Group Static Configuration Menu, type **s** to select the VLAN, then type **e**. Follow the instructions on the screen.

Enabling and Disabling Management Access

The IntraCore 8000 supports configurable management access for VLANs.

By default, management access is enabled, and all devices connected to the switch in a VLAN can communicate with the switch management agent.

▲ **Important:** You can disable management access for a VLAN. If security is a concern for members of a particular VLAN, disabling management access for that VLAN will prevent any member of that VLAN from attempting to change the switch's configuration. See "Enabling and Disabling Management Access."

To enable or disable management access for this VLAN, from the VLAN Group Static Configuration Menu, type **s** to select the VLAN, then type **t** to toggle management access.

Adding Port Members

To add ports as members of the VLAN, from the VLAN Group Static Configuration Menu, type **a**. Follow the instructions on the screen to enter the modules and ports to assign to the VLAN. Adding a port to a VLAN does not affect the port's status on any other VLAN.

Deleting Port Members

To delete ports as members of the VLAN, from the VLAN Group Static Configuration Menu, type **d**. Follow the instructions on the screen to enter the modules and ports to assign to the VLAN. Deleting a port from a VLAN does not affect the port's status on any other VLAN.

Moving Ports to This VLAN

To move ports to this VLAN, from the VLAN Group Static Configuration Menu, type **m**. Follow the instructions on the screen to enter the modules and ports to assign to the VLAN. Moving a port to a VLAN removes that port from any other VLAN on the switch.

Advanced Static VLAN Configuration

To access the Advanced Group Static Configuration Menu, type **v** in the VLAN Group Static Configuration Menu. A screen similar to Figure 4-8 appears.

```
IntraCore 8000 Advanced Group Static Config. Menu    VLAN Index: [01]
Module   Port List  1      8  9     16  17    24  25    32
======              ========  ========  ========  ========
  1  +: static      ++++++++  ++++++++  ++++++++  XXXXXXXX
  2  d: dynamic     ++++++++  ++++++++  ++++++++  XXXXXXXX
  3  -: Not Member  ++XXXXXX  XXXXXXXX  XXXXXXXX  XXXXXXXX
  4
  5
  6
  7
  8

VID: 0001    Created By: Mgmt      Name: Default VLAN
FID: 0000    Mgm Access: Enable    Status: Active, Independent

<Cmd>     <Description>          <Cmd>     <Description>
  a       Add Untagged Ports       d       Delete Untagged Ports
  v       Share This VLAN          i       Make This VLAN Independent
  m       Insert MAC Addr          r       Remove MAC Addr


Command>
Select VLAN    Next VLAN    Prev VLAN    Help    Quit
```

Figure 4-9 Advanced Group Static Configuration Menu

Current Settings

Table 4-6 describes each setting on the Advance Group Static Configuration Menu screen.

Setting	Description
VLAN Index	The VLAN Index of the VLAN group for which the information on the screen applies. The index is maintained by the system, and is not necessarily the same as the VID.
Port List	Shows each port's current membership status for this VLAN group.
VID	VLAN ID.
FID	Filtering ID.
Created By	Creator of this VLAN group; either Mgmt or GVRP.
Mgm Access	Whether management access is currently enabled or disabled.
Name	The name arbitrarily assigned to the VLAN group.
Status	Whether the VLAN group is active or inactive, and whether independent learning or shared learning of addresses is enabled.

Table 4-7 VLAN Group Static Configuration Settings

Specifying Tagging or No Tagging for a Port

Each VLAN maintains a list of ports that do not send tagged frames. When you add a port member to a VLAN, it is added to the untagged set by default. This means the frames sent out on this port will be untagged.

If you want to ristrict the port to sending only tagged frames on a given VLAN, you must delete the port from the VLAN's untagged set.

To delete a port from the untagged set, type **d** in the Advance Group Static Configuration Menu. Then enter the module and port description.

To add a port to the VLAN's untagged set, type **a** in the Advance Group Static Configuration Menu. Then enter the module and port description.

Specifying Shared or Independent Address Learning

By default, independent learning of addresses is enabled. Under independent learning, all addresses learned in a VLAN are stored in an address table for

that VLAN only, and all forwarding decisions for that VLAN are made by consulting that table. When shared learning is enabled, a single forwarding table is used by all VLANs that are members of the shared group. (For more information, see “Independent vs. Shared Learning.”)

To enable shared learning for a VLAN, type **v** in the Advance Group Static Configuration Menu. Then enter the index of the VLAN with which you want to share. You can repeat this procedure to share with multiple VLANs.

To enable independent learning for a VLAN, type **i** in the Advance Group Static Configuration Menu.

Inserting and Removing MAC Addresses

{{What does this do? What significance does inserting a MAC Address have for a VLAN? Help was no help. Still waiting for this info... The docs you sent me said nothing about inserting a MAC address, or single server/ multiple client.}}

To specify the MAC address for the station that {{what?}} for the VLAN, type type **m** in the Advance Group Static Configuration Menu, then specify the MAC address in the format **xx:xx:xx:xx:xx:xx** where **xx** is hexadecimal number separated by a colon.

To remove the MAC address from the VLAN, type type **r** in the Advance Group Static Configuration Menu, then specify the MAC address.

Configuring VLAN Port Attributes

To access the VLAN Port Configuration Menu, type v in the Configuration Menu to access the VLAN Management Menu, then type p to access the VLAN Port Configuration Menu. A screen similar to Figure 4-10 appears.

```
IntraCore 8000 VLAN Port Configuration Menu  Module Type: [24-100TX/RJ45]
Module: 01 Port: 01

Port VLAN Membership Info (+ : Member, -: Non Member):
VLAN Index :   1+--------  9--------- 17--------- 25---------
              33--------- 41--------- 49--------- 57---------

Port VLAN ID (PVID):    4095  Port GVRP Status:  Disabled
Port Frame Type: 802.1Q Tag   Port Ingress Filtering:  Disabled
Gvrp Failed Reg. Count: 0     Gvrp Last Pdu Origin : 00:00:00:00:00:00

<Cmd>     <Description>
  i       Set Port VLAN ID
  o       Add/Delete VLANs to/from Port
  f       Toggle Port Ingress Filtering Enable/Disable
  t       Toggle Port Receive Frame Type
  g       Toggle Port  GVRP Status
  q       Return to previous menu


Command>
Select Module Next module Prev module Select port Next port Prev port
```

Figure 4-10 VLAN Port Configuration Menu

Navigate to the module and port that you want to configure by typing a command as shown at the bottom of the screen.

Current Settings

Table 4-8 describes each setting on the GVRP Port Configuration Menu screen.

Setting	Description
Module	The IntraCore 8000 module for which the information on the screen applies.
Port	The port for which the information on the screen applies.
Port VLAN Membership Info	Shows each VLAN index's current membership status for this port.
Port VLAN ID (PVID)	This port's VLAN ID.
Port Frame Type	Whether the port currently receives all frames (tagged and untagged) or only 802.1Q tagged frames.
Gvrp Failed Reg. Count	The number of times the system has failed to dynamically register a VLAN. Failure usually indicates the maximum number of VLANS has been reached.
Port GVRP Status	Whether GVRP is currently enabled or disabled on this port.
Port Ingress Filtering	Whether ingress filtering is currently enabled or disabled on this port.
Gvrp Last Pdu Origin	The MAC address of the last Gvrp Pdu that was received.

Table 4-8 VLAN Port Configuration Settings

Setting the Port VLAN ID

Port VLAN ID (PVID) is used for VLAN classification of incoming untagged frames and has meaning only when a port is configured to receive both untagged and tagged frames. It is used to assign untagged frames to the VLAN identified by the PVID.

By default, each port on the switch has a PVID of 1 (the default VLAN). The allowed PVID range is 1 to 4094. For ports that are configured to receive only tagged frames, the PVID is meaningless and the port is assigned a PVID of 4095.

For ports that are members of more than one VLAN, received frames are assigned as follows:

- A tagged frame is forwarded to the VLAN matching the VID in the tag field of the frame
- An untagged frame is forwarded to the VLAN matching the PVID

To set the VLAN ID for the port, from the VLAN Port Configuration Menu, type **i**. Follow the instructions on the screen.

Adding and Deleting VLANs from the Port

To add VLANs to the port or delete VLANs from the port, from the VLAN Port Configuration Menu, type **o**. Follow the instructions on the screen.

Enabling and Disabling Port Ingress Filtering

By default, a port will accept and forward tagged frames whether or not the port is a member of a VLAN matching the VID of the tagged frame.

If ingress filtering is enabled, incoming tagged frames are forwarded only if the port is a member of the VLAN matching the VID of the tagged frame. All other frames are dropped and no addresses will be learned.

To enable or disable ingress filtering on the port, from the VLAN Port Configuration Menu, type **f** to toggle port ingress filtering.

Configuring Port Receive Frame Type

By default, all ports on the IntraCore 8000 receive both 802.1Q tagged frames and untagged frames. A port may be configured to receive only 802.1Q tagged frames. This configuration is a necessary part of Inter-Switch Link (ISL) configuration (see “Configuring Inter-Switch Links”).

If a port is configured to receive only tagged frames, any untagged frames received by the port are dropped and the source address of the untagged frames is not learned.

Incoming tagged frames are forwarded to the VLAN whose VID is included in the tag header of the frame. See “Enabling and Disabling Port Ingress Filtering” for more information about forwarding and filtering of received tagged frames.

To toggle the port between receiving all frames and receiving only tagged frames, from the VLAN Port Configuration Menu, type **t**.

Enabling and Disabling Port GVRP Status

To enable or disable GVRP on the port, from the VLAN Port Configuration Menu, type **g** to toggle the port's GVRP status.

- *Note:* For GVRP to be active, GVRP must be active for the system. See "Enabling and Disabling System GVRP" for instructions.

Configuring Inter-Switch Links

An inter-switch link (ISL) is a port that connects VLANs from two different switches; it's the means to share VLAN information between switches on a network.

To configure a port as an ISL, you must do the following:

- ❑ Add the ISL port to each VLAN that is shared by the two switches. This configures the port to share the VLAN traffic between the two switches.
- ❑ For each VLAN, remove the ISL port from the VLAN's set of untagged ports. By default, when you add a port to a VLAN, it will send tagged and untagged frames. This step configures the port to only send tagged frames.
- ❑ In most cases, configure the ISL port to receive tagged frames. A port that is configured to receive only tagged frames will drop untagged frames.

Once the port is configured as an ISL it will pass frames from switch to switch, but it can acts as a gate that only passes frames associated with specific VLANs.

Adding an ISL Port to VLANs

You add a port to a VLAN in the VLAN Static Group Configuration Menu.

1. Type **v** in the Configuration Menu to access the VLAN Management Menu, then type **s** to access the VLAN Group Static Configuration Menu.
2. Use the commands on the bottom of the menu to select the VLAN you want.

3. Once you select a VLAN, type **a**. Then enter the module and port to assign to the VLAN. You specify module and port separated by a colon. For example, **1:8** assigns port 8 of module 1.
4. Repeat steps 2 and 3 for each VLAN that is part of the ISL.

Configuring Tagging for the ISL Port on Each VLAN

You specify tagging for a port in the Advance Group Static Configuration Menu.

1. Type **v** in the Configuration Menu to access the VLAN Management Menu, then type **s** to access the VLAN Group Static Configuration Menu.
2. Use the commands on the bottom of the menu to select the VLAN you want.
3. Type **v** to display the Advance Group Static Configuration Menu.
4. Type **d**, then enter the module and port description for the ISL port. This removes the port from the VLAN's untagged set.

Configuring the ISL Port to Receive Tagged Frames

You configure a port to receive tagged frames in the VLAN Port Configuration Menu.

1. Type **v** in the Configuration Menu to access the VLAN Management Menu, then type **p** to access the VLAN Port Configuration Menu.
2. Use the commands on the bottom of the menu to select the module and port you want.
3. To toggle the port between receiving all frames and receiving only tagged frames, from the VLAN Port Configuration Menu, type **t**.

Displaying a Summary of VLAN Groups

To view a summary of VLAN groups, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **d** to access the VLAN Group Summary. A screen similar to Figure 4-11 appears.

```
IntraCore 8000 VLAN Groups Summary
+-----+-------+-----------+------------+------+--------------------+
|Index|VLAN ID|Mgmt Access| Created By | FID  | Status             |
+-----+-------+-----------+------------+------+--------------------+
   1        1   Enable      Mgm Action    0     Active, Independent
   2     1024   Enable      Mgm Action    1     Active, Independent


End of VLAN Summary,   Quit
```

Figure 4-11 VLAN Groups Summary

Displaying a VLAN Port Summary

To view a module port VLAN summary, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **m** to access the Module Port VLAN Summary. A screen similar to Figure 4-12 appears.

```
IntraCore 8000 Module 1 Port VLAN Info

======+======+============+==========+
 Port | PVID |   Tx/Rx    | Ingress  |
Number|      | Frame Type |Filtering |
======|======|============|==========|
   1  | 4095 | 802.1Q Tag | Disabled |
   2  | 0001 | All Frames | Disabled |
   3  | 0001 | All Frames | Disabled |
   4  | 0001 | All Frames | Disabled |
   5  | 0001 | All Frames | Disabled |
   6  | 0001 | All Frames | Disabled |
   7  | 0001 | All Frames | Disabled |
   8  | 0001 | All Frames | Disabled |
   9  | 0001 | All Frames | Disabled |
  10  | 0001 | All Frames | Disabled |
  11  | 0001 | All Frames | Disabled |
  12  | 0001 | All Frames | Disabled |
  13  | 0001 | All Frames | Disabled |
  14  | 0001 | All Frames | Disabled |
  15  | 0001 | All Frames | Disabled |
  16  | 0001 | All Frames | Disabled |

Quit  Next Page  Select Module  Previous Module  neXt Module
```

Figure 4-12 Port VLAN Info screen

To view the summary for other modules, type a command as shown at the bottom of the screen.

Displaying a VLAN FID-VID Association Summary

To view a summary of the FIDs and their associated VIDs, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **f** to access the VLAN FID-VID Association summary. A screen similar to Figure 4-13 appears.

```
IntraCore 8000 FID Summary
+-----+-------------------------------------------------------------+
  FID |                          VIDs                               |
+-----+-------------------------------------------------------------+
  00  | 001
+-----+-------------------------------------------------------------+
  01  | 1024
+-----+-------------------------------------------------------------+
```

Figure 4-13 VLAN FID-VID association summary

Resetting VLAN Configuration to Defaults

To reset the security measures on the IntraCore 8000 to the factory defaults, access the VLAN Management Menu by typing **v** in the Configuration Menu. Then type **r** to reset all of the VLAN configurations that have been changed back to the factory-set defaults.

Configuring GVRP

GARP VLAN Registration Protocol (GVRP) allows an above-end station to to be registered as wanting to join a specific VLAN. This creates a dynamic VLAN topology that responds to VLAN traffic; until it sees activity from the specific VLAN, the registered station doesn't appear to be part of that VLAN.

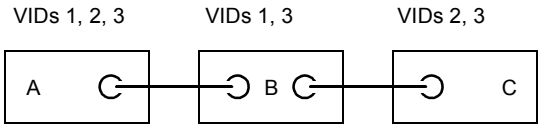


Figure 4-14 A three-switch network with VLANs 1, 2, and 3

For example, assume a three-switch network that includes three VLANs; VID 1, VID 2, and VID 3. Also assume that the switches (A, B, and C) are configured with the VLAN groups shown in Figure 4-14. In this case, switch A and switch C both include VLAN #2 in their VLAN groups. However, the VLAN traffic must cross switch B.

Using GVRP, switches A and C can register their interest in VLAN #2 with switch B. Then switch B can join the VLAN #2 topology when it receives frames tagged with that VID. Once it does, it can then pass that VLAN traffic to switches A and C.

To access the GVRP Configuration Menu, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **g** to access the GVRP Configuration Menu. A screen similar to Figure 4-15 appears.

```
IntraCore 8000 GVRP Configuration Menu  System GVRP:  Disabled

VLAN[1] Id : 1 Dynamic Port Map

Module   Port List  1      8  9     16  17    24  25    32
======              ========  ========  ========  ========
  1  +: Member      --------  --------  --------  XXXXXXXX
  2  -: Not Member  --------  --------  --------  XXXXXXXX
  3                 --XXXXXX  XXXXXXXX  XXXXXXXX  XXXXXXXX
  4
  5
  6
  7
  8

<Cmd>     <Description>
  t       Toggle System GVRP Status
  e       Enable GVRP on Group of Ports
  d       Disable GVRP on Group of Ports
  f       Forbidden Set Configuration
  r       Regisration Fixed Set Configuration

Command>
Select VLAN     Next VLAN     Previous VLAN          Quit
```

Figure 4-15 GVRP Configuration Menu

Navigate to the VLAN that you want to configure by typing a command as shown at the bottom of the screen.

Current Settings

Table 4-9 describes each setting on the GVRP Configuration Menu screen.

Setting	Description
System GVRP	Whether GVRP is currently enabled or disabled on the system.
VLAN ID	The VLAN ID of the VLAN group for which the information on the screen applies.
Port List	Shows the current membership status of each port to this VLAN group.

Table 4-9 GVRP Configuration Settings

Enabling and Disabling System GVRP

To enable or disable GVRP on the IntraCore 8000, from the GVRP Configuration Menu, type **t** to toggle the status of system GVRP.

Enabling GVRP on a Group of Ports

To enable GVRP on a group of ports, from the GVRP Configuration Menu, type **e**.

Disabling GVRP on a Group of Ports

To disable GVRP on a group of ports, from the GVRP Configuration Menu, type **d**.

Configuring VLAN Forbidden Sets

Each switch keeps a list of ports that are not to be added to a VLAN by GVRP. You specify the set of forbidden portsper VLAN. To access the VLAN Forbidden Set Configuration Menu, type **f** from the GVRP Configuration Menu. A screen similar to Figure 4-16 appears. Use the commands at the bottom of the menu to select a VLAN.

```
IntraCore 8000 VLAN Forbidden Set Configuration Menu   VLAN Index: [01]

Module   Port List  1      8  9     16  17    24  25    32
======              ========  ========  ========  ========
  1  +: Member      --------  --------  --------  XXXXXXXX
  2  -: Not Member  --------  --------  --------  XXXXXXXX
  3                 --XXXXXX  XXXXXXXX  XXXXXXXX  XXXXXXXX
  4
  5
  6
  7
  8
<Cmd>     <Description>
  a       Add ports to Forbidden Set
  d       Delete ports from Forbidden Set


Command>
Select VLAN     Next VLAN     Previous VLAN          Quit
```

Figure 4-16 VLAN Forbidden Set Configuration Menu

1. Use the commands at the bottom of the menu to select a VLAN.
2. Type **a** to add a list of ports to the forbidden set, or type **d** to delete a list of ports from the forbidden set. Then follow the instructions.

Configuring Registration Fixed Sets

To access the VLAN Registration Fixed Set Configuration Menu, type **r** from the GVRP Configuration Menu. A screen similar to Figure 4-17 appears.

```
IntraCore 8000 VLAN Fixed Set Configuration Menu   VLAN Index: [01]

Module   Port List  1      8  9     16  17    24  25    32
======              ========  ========  ========  ========
  1  +: Member      --------  --------  --------  XXXXXXXX
  2  -: Not member
  3
  4

 <Cmd>     <Description>
  a       Add ports to Forbidden Set
  v       Delete ports from Forbidden Set




Command>
Select VLAN     Next VLAN     Prev VLAN      Help      Quit
```

Figure 4-17 VLAN Registration Fixed Set Configuration Menu

{{This is incomplete. Needs more GVRP info - waiting for Breen.}}

Multicast Traffic Management

Multicast traffic is a means to transmit a multimedia stream from the internet (a video conference, for example) without requiring a TCP connection from every remote host that wants to receive the stream. The stream is sent to the multicast address, and from there it's propegated to all interested parties on the internet.

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts (group transmission).

Multicast Addresses

Multicasts are sent to special IP addresses in the range from 224.0.0.0 through 239.0.0.0. These are also called "Class D" addresses. The IP multicast address always begins with the four bits 1110 (which identifies the address as a multicast). The remaining 28 bits of the multicast address specify the individual multicast group.

When an end station wants to join in a multicast group, it binds the multicast address of that group to its network interface. When a node is using an IP multicast address it also uses an ethernet multicast address. Ethernet IP multicast addresses begin 01:00:5e. The remaining 24 bits are the lowest 24 bits of the IP multicast address. (However, there is not a 1-to-1 mapping of IP multicast addresses to Ethernet multicast addresses.)

When configuring a VLAN for multicast traffic, you specify the ehternet address for the multicast group. (See "Multicast Forwarding Database Configuration".)

IGMP

Communication on a LAN between end stations and routers is managed by the Internet Group Management Protocol (IGMP). For complete information about IGMP, see RFC 1112, "Host Extensions..." and RFC 2236, "Internet Group Management Protocol, Version 2" <ftp://ftp.isi.edu/in-notes/rfc2236.txt>

A router that supports multicast and IGMP sends periodic messages called "queries" on its LAN interfaces. These queries inquire if any end stations want to join a multicast group. End stations signal their desire to join the multicast group by responding with an IGMP "report". By using a multicast

routing protocol, such as Protocol-Independent Multicast (PIM), routers maintain forwarding tables that they use to forward multicast datagrams.

Packets delivered to members of the multicast group are identified by a single multicast group address. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

IGMP Snooping

A traditional layer-2 switch is unable to determine which end stations on the LAN are interested in which multicast groups. To avoid unnecessary flooding, the switch may use IGMP Snooping. That means the switch listens to IGMP messages to learn which ports want multicast traffic from which multicast groups. The switch inserts the correct Ethernet multicast address into the forwarding table for the ports where an end station has joined a multicast group.

GMRP - GARP Multicast Registration Protocol

A limitation of IGMP Snooping is that all IP multicast traffic must be examined to build the tables necessary to prune the multicasts. GMRP, an IEEE standard, provides a mechanism for end stations to directly inform a switch of its interest in a particular multicast group.

When it wants to join a group, an end station sends a GARP packet to the GMRP multicast address, 01:80:00:00:20. Switches that support GMRP use such GARP packets to notify routers of the presence of group members, and to configure their forwarding tables to avoid unnecessary flooding.

- *Note:* GMRP operates at layer 2, while IGMP is an IP protocol and operates at layer 3.

For more information about GMRP, see ANSI/IEEE Std. 802.1D -- 1998 Edition, which includes the 802.1p standard. See <http://www.ieee.org> for more information.

IP Multicast Quality of Service - RSVP

The IntraCore 8000 also supports the industry standard Resource Reservation Protocol (RSVP). RSVP allows an end station to reserve resources across the net in an attempt to maintain quality of service from a multicast provider. The IntraCore 8000 monitors RSVP messages so it can

set its priority queues to the correct values for the Quality of Service requested.

For more information about RSVP, see RFC 2205 -- Resource ReserVation Protocol (RSVP) -- Version 1 Functional Specification <ftp://ftp.isi.edu/rfc2205.txt>

Configuring Multicast Traffic Management

The Multicast Traffic Management Menu allows you to set up group transmission. To access the Multicast Traffic Management Menu, type c in the Configuration Menu. A screen similar to Figure 4-18 appears.

```
IntraCore 8000 Multicast Traffic Management Menu

Multicast Forwarding Database
-----------------------------
Multicast Group Address Count    : 0

GMRP Status                      : Disabled
IGMP Snooping                    : Disabled
Multicast Policy[RSVP]-based QOS : Disabled

<Cmd>     <Description>
  g       Toggle GMRP Status Enable/Disable
  i       Toggle IGMP Snooping Enable/Disable
  p       Toggle Multicast Policy-based QOS Enable/Disable
  m       Multicast Forwarding Database Configuration
  d       Display All Group Addresses
  q       Return to previous menu




Command>
```

Figure 4-18 Multicast Traffic Management Menu

Current Settings

Table 4-10 describes each setting on the Multicast Traffic Management Menu.

Setting	Description
Multicast Group Address Count	The number of multicast group addresses in the forwarding table.
GMRP Status	Whether GMRP is enabled or disabled.
IGMP Snooping	Whether IGMP Snooping is enabled or disabled.
Multicast Policy [RSVP]-based QOS	Whether 'RSVP]-based QOS is enabled or disabled.

Table 4-10 Multicast Traffic Management Settings

Enabling and Disabling GMRP

To enable or disable GMRP on the IntraCore 8000, from the Multicast Traffic Management Menu, type g to toggle the status of system GMRP.

Enabling and Disabling IGMP Snooping

To enable or disable IGMP Snooping on the IntraCore 8000, from the Multicast Traffic Management Menu, type i to toggle the status of IGMP Snooping.

Enabling and Multicast Poliocy-based Quality of Service

To enable or disable QOS on the IntraCore 8000, from the Multicast Traffic Management Menu, type p to toggle the status of QOS.

Displaying a Summary of Group Addresses

To display a list of multicast group addresses, from the Multicast Traffic Management Menu, type d. A screen similar to Figure 4-19 appears.

```
+-------------------+-------+-----+-------------------
| Group MAC Address |  VID  | Pri | Action
+-------------------+-------+-----+-------------------
  01:00:5E:12:34:56    0001    0    Mgm Action
  01:00:5E:78:90:12    0001    0    Mgm Action



End of Summary,             Quit
```

Figure 4-19 Summary of Group Addresses

Multicast Forwarding Database Configuration

The Multicast Forwarding Database lists addresses of multicast groups, and assigns them to specific VLANs. It also lists the ports within a VLAN that are can receive traffic from the multicast address.

To access the Multicast FDB Configuration Menu, type c in the Configuration Menu to display the Multicast Traffic Management Menu. Then type **m**. A screen similar to Figure 4-20 appears.

```
IntraCore 8000 Multicast FDB Configuration Menu    VLAN Index: [01]

Multicast Group Address:  01:00:5E:12:34:56
Created By:               Mgm Action
Priority:                 0


<Cmd>     <Description>
  o       Add/Delete Ports
  h       Help
  q       Return to previous menu


Command>
Select VLAN  Select Addr  Next Addr  Prev Addr  Insert Addr  Remove Addr
```

Figure 4-20 Multicast FDB Configuration Menu

Use the commands at the bottm of the menu to select a VLAN or Multicast Group address.

Adding ports to the Selected Address

To add or delete ports belonging to the multicast group:

1. Select the VLAN that contains the ports and the address. Type **v** and follow the instructions.
2. Select the Multicast Group address. Type **s** and follow the instructions.
3. Type **o** and follow the instructions.

Inserting a Multicast Group Address

Inserting an address adds the address to the list of Multicast Groups for the current VLAN. The addresses begin 01:00:5e. The remaining 24 bits are the lowest 24 bits of the IP multicast address.

To add an address:

1. Select the VLAN to which you will assign the new address. Type **v** and follow the instructions.
2. Type **i** and follow the instructions to add the new address.

Removing a Multicast Group Address

To remove an address:

1. Select a VLANfrom which you will remove the address. Type **v** and follow the instructions.
2. Type **r** and follow the instructions to remove the address.

5
Web Browser Management

This chapter tells how to manage the IntraCore 8000 by means of a Web browser, using Web pages to monitor and configure the switch.

Most of the options and functions provided by Web browser management are similar to those of the Local Management Interface. For additional details about managing the IntraCore 8000, refer to Chapter 3, "Configuration," and Chapter 4, "Advanced Management."

- *Note:* The Web Browser interface to the IntraCore 8000 is disabled by default. You enable the Web Browser interface in the User Interface Configuration Menu (see "User Interface Configuration").

Accessing with a Web Browser

This section explains how to access the HTTP server and view the management features it offers. To use Web browser management, the IntraCore must be configured with an IP address. For instructions on configuring IntraCore with an IP address, see Chapter 2, "Configuring for Management,"

1. Locate a computer with a functioning World Wide Web browser and open the browser.
2. Type the switch IP address at the URL prompt.
3. Enter user name IntraCore and a password. The password is the same as the current console password. (The default password is **Asante**.)
4. Press Return. The Web Browser Management Overview page appears, as shown in Figure 5-1.

   - *Note:* The browser pages shown in this chapter are typical of those used for the IntraCore and settings are given only as examples. The user must configure the IntraCore with parameters that are specific to the user's application and site requirements.

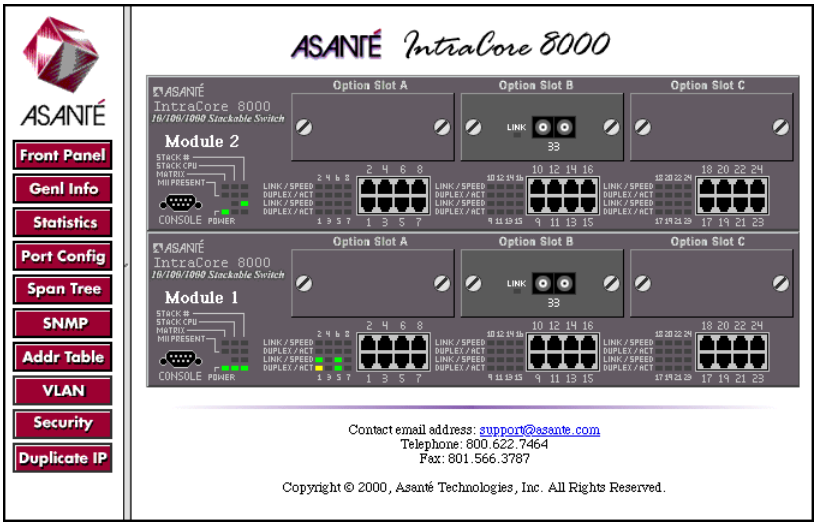


Figure 5-1 Web Browser Management Overview page

The Web Browser Management Overview page contains a sidebar with nine management option buttons, and a view of the IntraCore front panel that displays real-time IntraCore 8000 operating information.

Management Buttons

The buttons on the left provide the following options:

- ❑ Front Panel
- ❑ Genl Info (General Information)
- ❑ Statistics
- ❑ Port Config (Port Configuration)
- ❑ Span Tree (Spanning Tree Protocol Configuration)
- ❑ SNMP (Simple Network Management Protocol)
- ❑ Addr Table (IP/MAC Address Table)
- ❑ VLAN (Virtual LAN Configuration)
- ❑ Duplicate IP (Duplicate IP Trap Log)

The following sections describe and explain the pages that are displayed when you click each of the buttons.

Front Panel Button

This button opens (or refreshes) the Web Browser Management Overview page. This is the top-level or opening page. The Web Browser Management Overview page is shown in Figure 5-1 and contains the following elements:

- ❑ Front panel display
- ❑ Port activity indicator
- ❑ Port selector feature

Front Panel Display

The front panel graphic displays the image of the connected switch, its LED panel, and the active data ports.

Port Activity Indicator

The front panel LED display simulates the IntraCore in real-time operating mode. It approximates all switch activity as it occurs.

Port Selector Feature

If you point the cursor to a port connector and click the mouse, a port-specific page is displayed, which shows the selected port's configuration and traffic statistics.

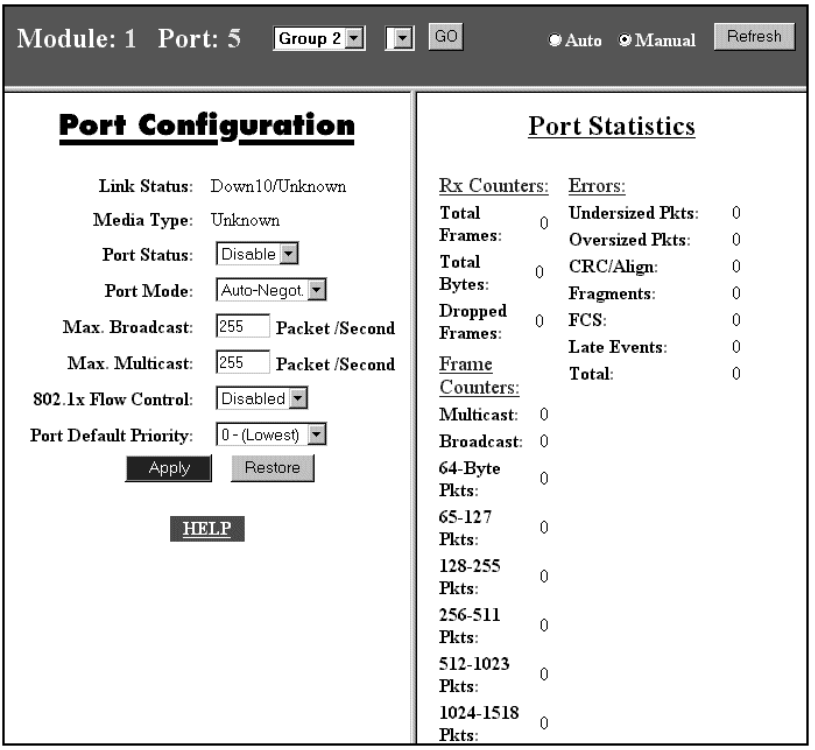


Figure 5-2 Port Configuration and Statistics page

GenI Info (General Information) Button

This button opens the IntraCore's General Information page. The page has six sub-levels, which are listed at the top of Figure 5-3. The General Information fields are described fully in "User Interface Configuration" in Chapter 3.

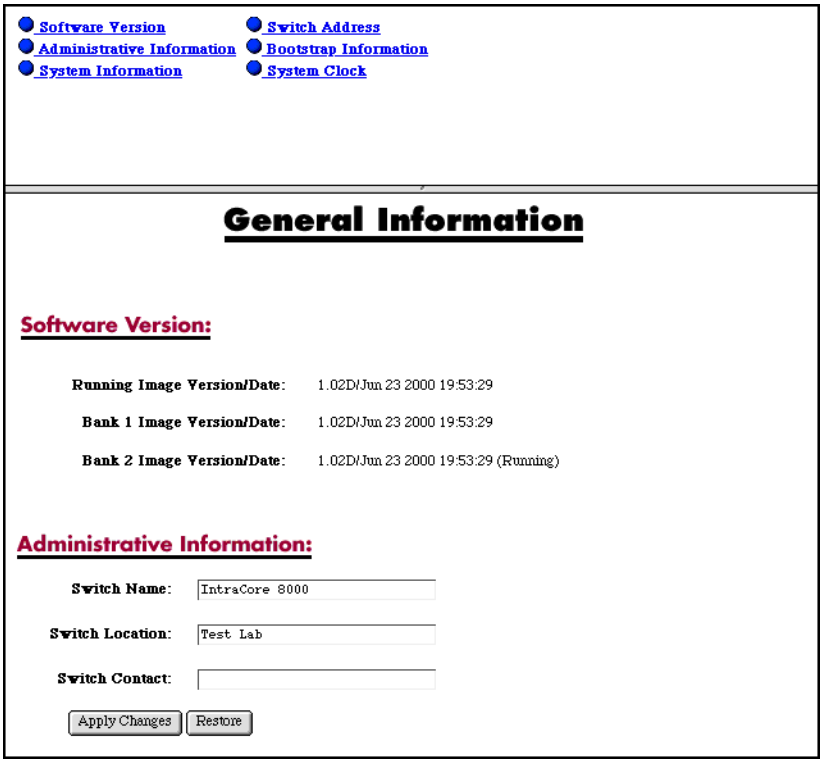


Figure 5-3 General Information page

The first two sub-levels, Software Version and Administrative Information, are displayed on the opening page. To view the other sub-levels, click the links for them at the top of the General Information page.

Statistics Button

This button opens the Statistics page, which presents a graphical image of the IntraCore statistics, as shown in Figure 5-4. On this page, the user can view system statistics since the last system reset. For a description of the statistics counters, see “Viewing Statistics” on page 3-52.

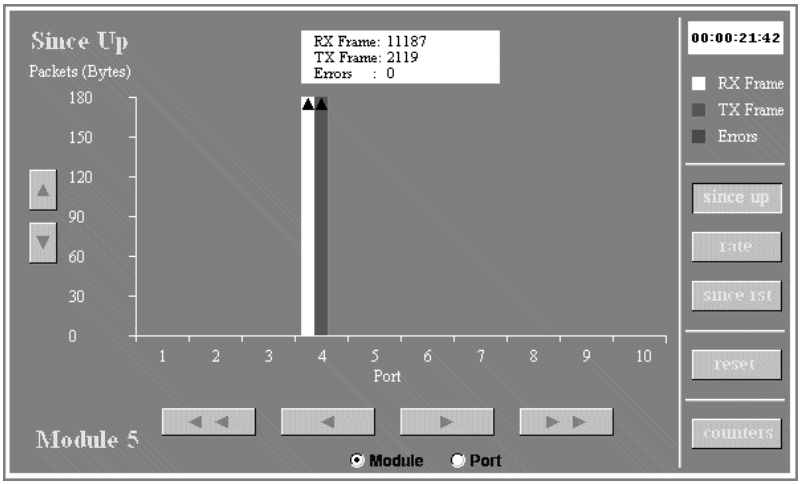


Figure 5-4 Statistics - Bar Chart

The following features allow you to modify the statistics bar chart.

- Up-Down Arrows – The left-most up and down arrows let you scroll the screen up to view the counter graph. This is useful when the counters have run off the screen due to the system having been up for a long time.
- Right-Left Arrows - These arrows beneath the Bar Chart let you view the statistics for different ports on the same module (if the Port radio button is selected) or ports in different modules (if the Module radio button is selected).
- Since Up Button – Brings up a graph of the total packets/bytes switched on the ports since the switch was last reset or powered on.
- Rate Button – Displays the rate of the packets or bytes per port.
- Since Rst – Displays the packets/bytes switched since the manage-

ment counters were last reset or cleared.

- ❑ Reset – Clears the counters for future samplings.
- ❑ Counters – Displays the statistical counters of the associated view, since up or since reset, as shown in Figure 5-6 and Figure 5-7.

◆ *Note:* You may also view a summary of the frames per port by placing the cursor on the desired bar. A box with the statistics appears, as shown in

To see either a line graph or a table display of the system's statistics, click on a bar, then choose the option you want from the pop-up menu at the top of the Statistics page, and click **Apply**.

In Figure 5-5, the Received Frames statistics for a single port are displayed in a line graph.

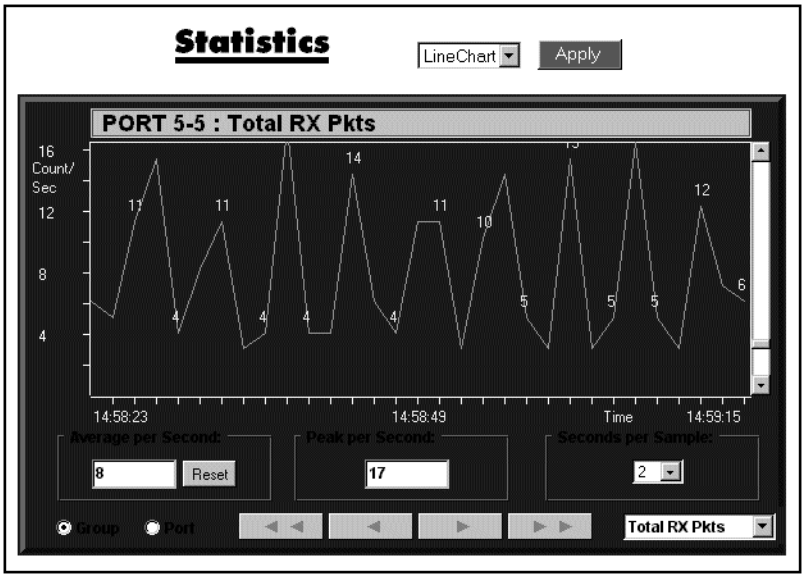


Figure 5-5 Line chart of received frames for a port

In Figure 5-6, a summary of the counters for a port is displayed in table format.

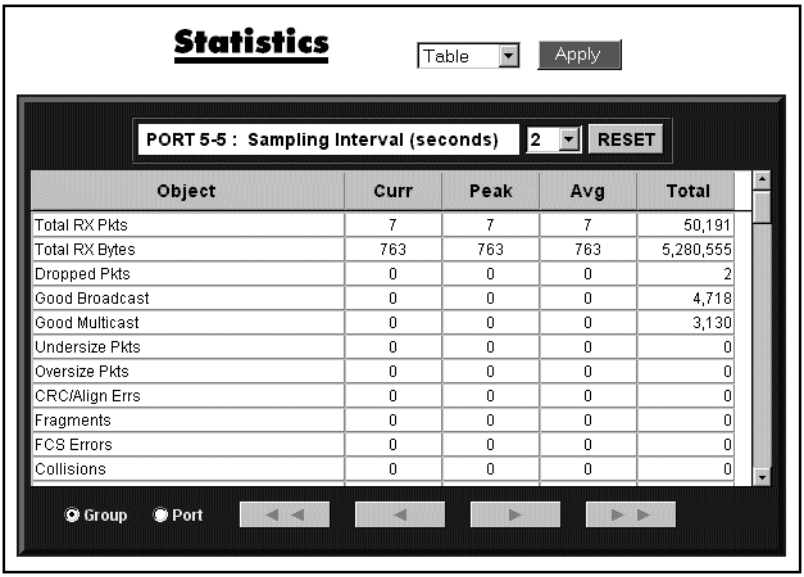


Figure 5-6 Summary of counters for a port

In Figure 5-7 the counters for a port are displayed in bar graph form.

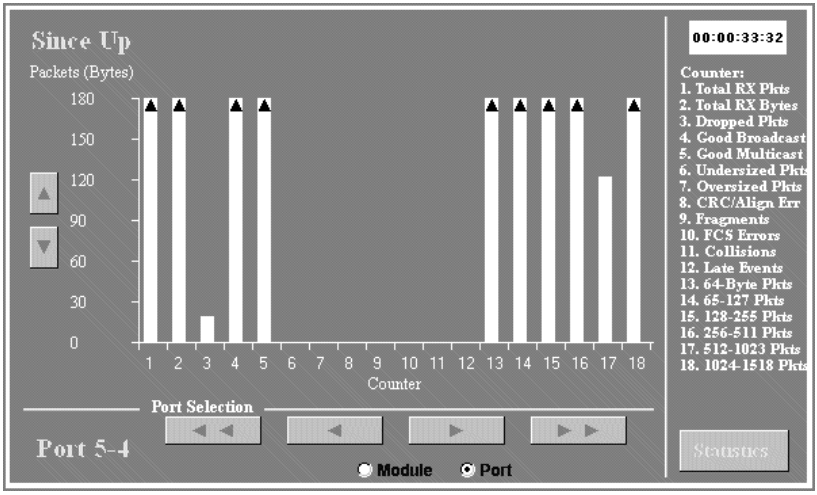


Figure 5-7 Bar graph of counters for a port

Port Config (Port Configuration) Button

This button opens the Port Configuration page, which provides a comprehensive overview of the status of each port on the IntraCore, as shown in Figure 5-8. The configuration page for any individual port can be accessed by single clicking on the associated blue number in the right or left hand margin.

Port Configuration

- Click on the Module - Port number to go to the port configuration setting page

Module 2 Module 5

Module - Port	State	Port status	Link status	Type	Mode	Module - Port
5 - 1	Forwarding	Enabled	Down	TX	100/FULL	5 - 1
5 - 2	Forwarding	Enabled	Down	TX	100/FULL	5 - 2
5 - 3	Forwarding	Enabled	Down	TX	100/FULL	5 - 3
5 - 4	Forwarding	Enabled	Down	TX	100/FULL	5 - 4
5 - 5	Forwarding	Enabled	Up	TX	10/Half	5 - 5
5 - 6	Forwarding	Enabled	Down	TX	100/Half	5 - 6
5 - 7	Forwarding	Enabled	Down	TX	100/Half	5 - 7
5 - 8	Forwarding	Enabled	Down	TX	100/Half	5 - 8
5 - 9	Forwarding	Enabled	Down	TX	100/Half	5 - 9
5 - 10	Forwarding	Enabled	Down	TX	100/Half	5 - 10
5 - 11	Forwarding	Enabled	Down	TX	100/Half	5 - 11
5 - 12	Forwarding	Enabled	Down	TX	100/Half	5 - 12
5 - 13	Forwarding	Enabled	Down	TX	100/Half	5 - 13
5 - 14	Forwarding	Enabled	Down	TX	100/Half	5 - 14
5 - 15	Forwarding	Enabled	Down	TX	100/Half	5 - 15
5 - 16	Forwarding	Enabled	Down	TX	100/Half	5 - 16
5 - 17	Forwarding	Enabled	Down	TX	100/Half	5 - 17
5 - 18	Forwarding	Enabled	Down	TX	100/Half	5 - 18
5 - 19	Forwarding	Enabled	Down	TX	100/Half	5 - 19
5 - 20	Forwarding	Enabled	Down	TX	100/Half	5 - 20
5 - 21	Forwarding	Enabled	Down	TX	100/Half	5 - 21
5 - 22	Forwarding	Enabled	Down	TX	100/Half	5 - 22
5 - 23	Forwarding	Enabled	Down	TX	100/Half	5 - 23
5 - 24	Forwarding	Enabled	Down	TX	100/Half	5 - 24
Module - Port	State	Port status	Link status	Type	Mode	Module - Port

Figure 5-8 Port Configuration table

To view the Port Configuration table for the ports of a different module, click on the module number link at the top of the table. For example in Figure 5-8, you could see the table for the ports in Module 2 by clicking on the Module 2 link at the top of the table.

Span Tree (Spanning Tree) Button

This button opens the Spanning Tree Protocol (STP) Configuration page, which shows the STP Configuration of the IntraCore, as shown in Figure 5-9. STP configuration is explained in Chapter 4, “Advanced Management.” Click the STP Port Configuration button to display the STP Configuration settings for each port.

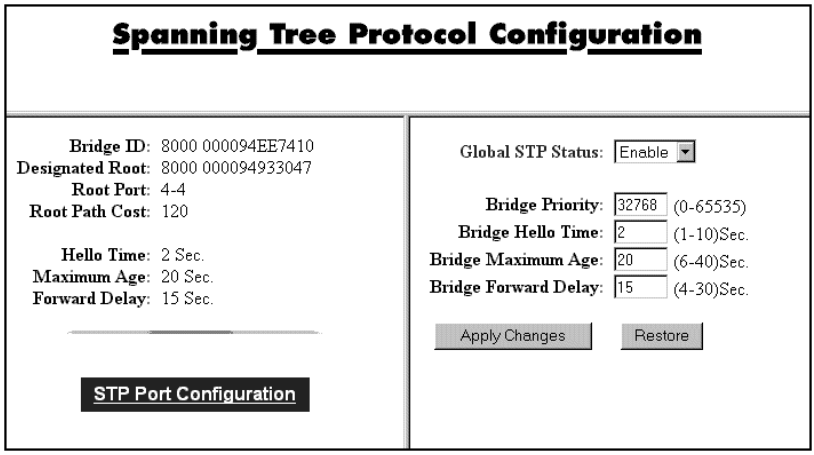


Figure 5-9 Spanning Tree Configuration page

▲ **Important:** Do NOT configure any STP parameters unless you have knowledge of and experience with the IEEE 802.1d specification.

SNMP Button

This button displays the SNMP (Simple Network Management Protocol) page, as shown in Figure 5-10. See “SNMP Configuration” in Chapter 3 for an explanation of SNMP settings.

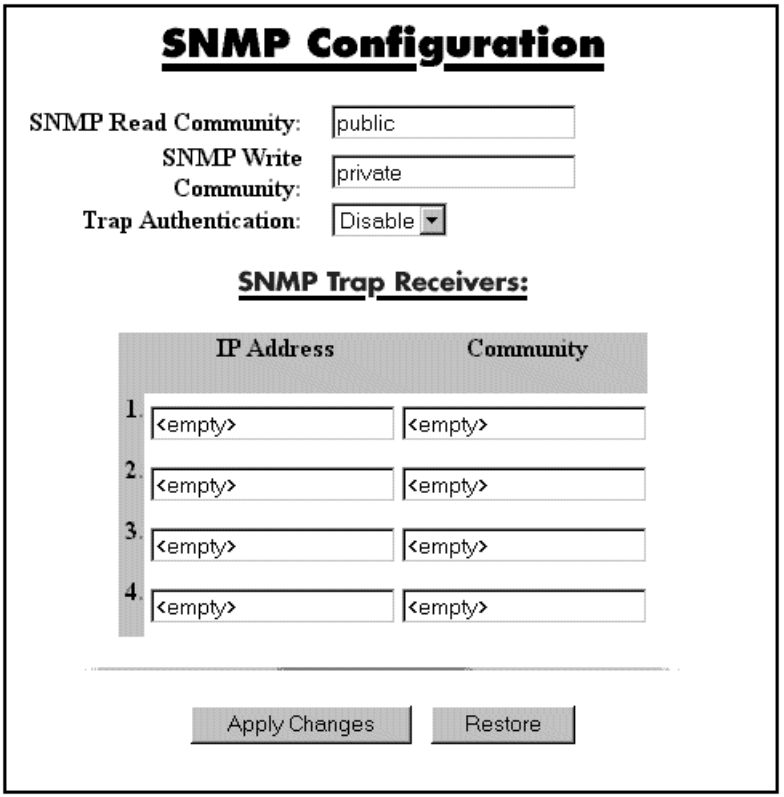
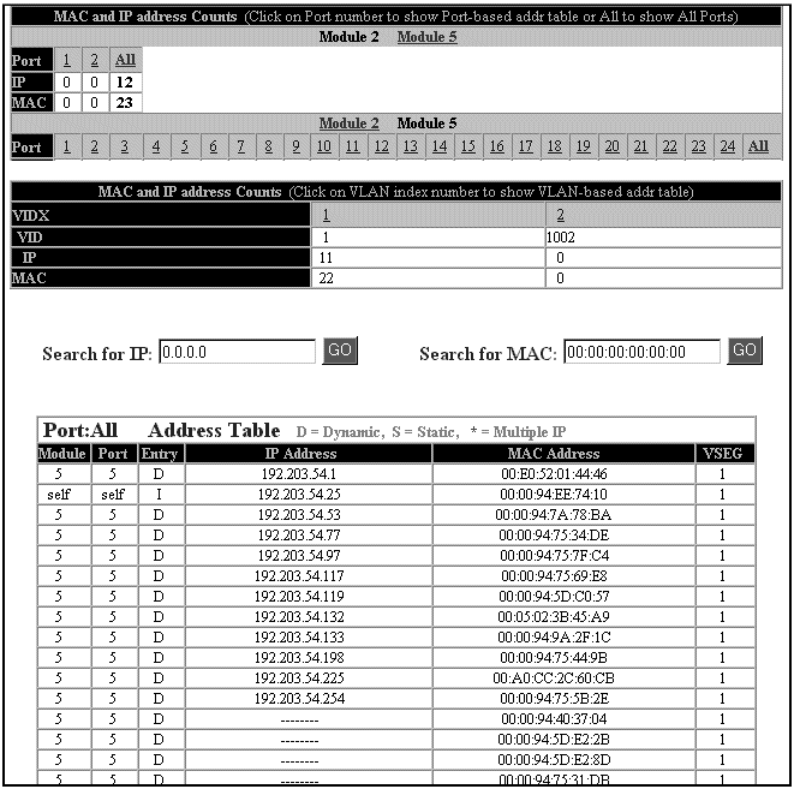


Figure 5-10 SNMP Configuration page

Addr (Address) Table Button

The Addr Table button opens the MAC and IP Address Table page, which displays two tables, as shown in Figure 5-11. The top table displays the counts of IP and MAC addresses for each port. The lower table displays IP and MAC addresses for either a particular port, or all ports. The display for all ports is shown in Figure 5-11. The activity status (Entry) and VLAN segment (VSEG) are also displayed for each device.



MAC and IP address Counts (Click on Port number to show Port-based addr table or All to show All Ports)

Module 2 Module 5

Port	1	2	All
IP	0	0	12
MAC	0	0	23

Module 2 Module 5

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	All

MAC and IP address Counts (Click on VLAN index number to show VLAN-based addr table)

VIDX	1	2
VID	1	1002
IP	11	0
MAC	22	0

Search for IP: 0.0.0.0 GO Search for MAC: 00:00:00:00:00:00 GO

Port:All Address Table D = Dynamic, S = Static, * = Multiple IP

Module	Port	Entry	IP Address	MAC Address	VSEG
5	5	D	192.203.54.1	00:E0:52:01:44:46	1
self	self	I	192.203.54.25	00:00:94:EE:74:10	1
5	5	D	192.203.54.53	00:00:94:7A:78:BA	1
5	5	D	192.203.54.77	00:00:94:75:34:DE	1
5	5	D	192.203.54.97	00:00:94:75:7F:C4	1
5	5	D	192.203.54.117	00:00:94:75:69:E8	1
5	5	D	192.203.54.119	00:00:94:5D:C0:57	1
5	5	D	192.203.54.132	00:05:02:3B:45:A9	1
5	5	D	192.203.54.133	00:00:94:9A:2F:1C	1
5	5	D	192.203.54.198	00:00:94:75:44:9B	1
5	5	D	192.203.54.225	00:A0:CC:2C:60:CB	1
5	5	D	192.203.54.254	00:00:94:75:5B:2E	1
5	5	D	--------	00:00:94:40:37:04	1
5	5	D	--------	00:00:94:5D:E2:2B	1
5	5	D	--------	00:00:94:5D:E2:8D	1
5	5	D	--------	00:00:94:75:31:DB	1

Figure 5-11 MAC and IP Address Table page

To see the MAC and IP addresses, the activity status, and the VLAN segment for the devices connected to a particular port, click the port's number in the top table. Use the Search boxes to search for either an IP or MAC address on the IntraCore.

VLAN Button

This button opens the VLAN Groups page, as shown in Figure 5-12. The page shows the modules of the IntraCore 8000, and the ports that are assigned to the currently selected VLAN. There is also a panel that shows the VID of each VLAN on the current switch; to select a VLAN, click the appropriate VID. For information about VLANs, see Chapter 4.

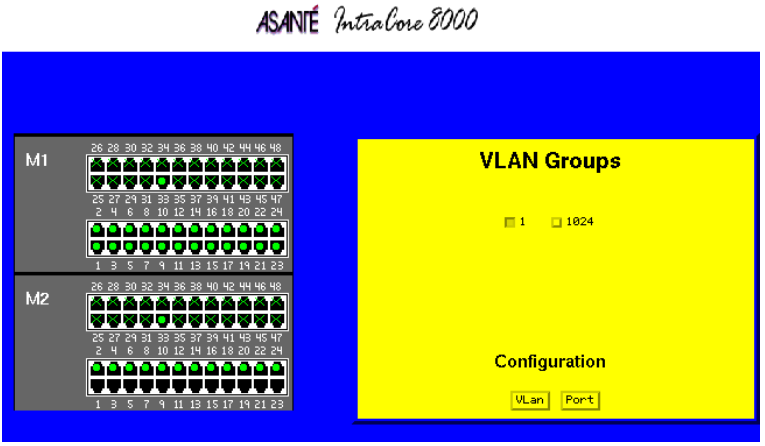


Figure 5-12 VLAN Groups page

To configure the selected VLAN, click the **VLAN** button. To configure the ports for the selected VLAN, click the **Ports** button.

Port Configuration

Clicking the **Ports** button in the VLAN Groups page opens the VLAN Port Selection page, as shown in Figure 5-13. The page shows the modules of the IntraCore 8000. There is also a panel indicating the current Port VLAN ID and its settings.

To see and modify the settings for a port, click on the connector for it in the module simulation. Then make the appropriate settings in the right-hand panel of the page.

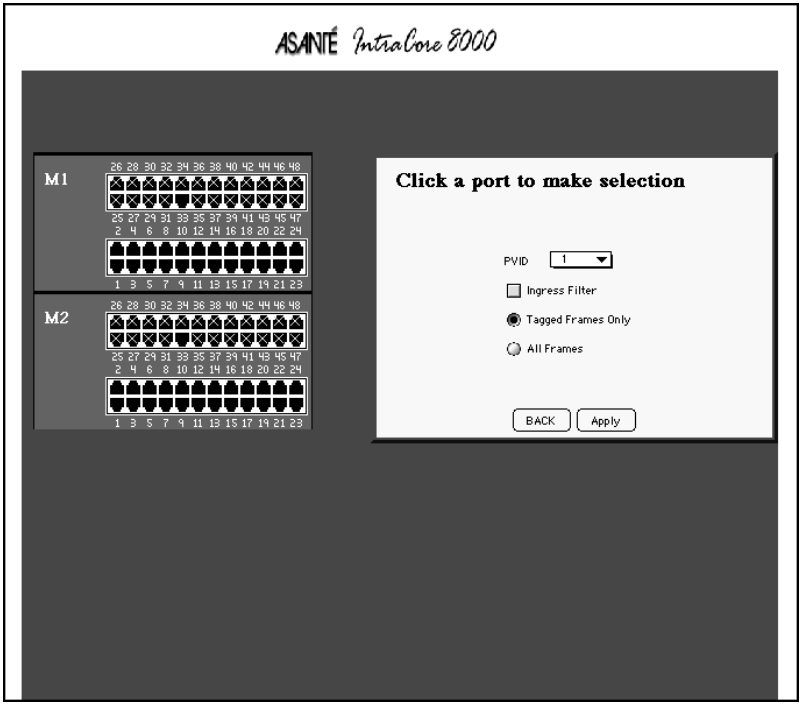


Figure 5-13 VLAN Port Selection page

VLAN Configuration

To congigure a VLAN, first select a VIDin the VLAN Groups page (Figure 5-12), then click the **VLAN** button. This opens the VLAN Group Configuration options page, as shown in Figure 5-14.

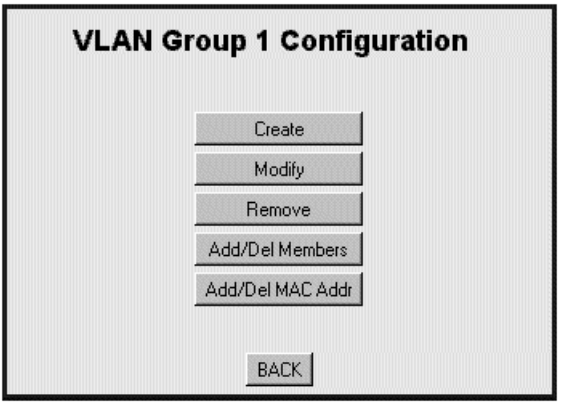


Figure 5-14 VLAN Group Configuration options

Creating or Modifying a VLAN

To create or modify the basic attributes of a VLAN group, click the **Create** or **Modify** button in the VLAN Group Configuration dialog box. The VLAN Attributes dialog box is displayed, as shown in Figure 5-15.

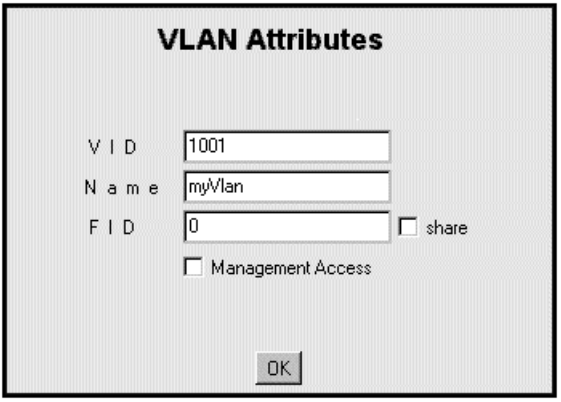


Figure 5-15 VLAN Attributes dialog box

Enter or change the basic attributes, then click OK.

Removing a VLAN

To remove a VLAN from the current switch, click Remove in the VLAN Group Configuration dialog box. This removes the VLAN you selected at

the time you clicked VLAN in the VLAN Groups dialog page (Figure 5-12). You will see a dialog box asking you to confirm your decision to remove the VLAN.

{{The above is total fiction. Is it right?}}

Adding and Deleting Port Members

To add ports to or delete ports from the current VLAN, click the Add/Del Members button in the VLAN Group Congiguration dialog box. This displays the Add/Delete Port Member dialog box, as shown in Figure 5-16.

In the right-hand panel you can select to show the ports that are in the untagged set or the tagged set of the VLAN. These ports appear in the module simulation on the left. Darkened ports are not members, ports with a green X are untagged members, and ports with a green dot are tagged members.

To modify the port members:

1. Select the action you want to perform in the right-hand panel; Add/Delete Port Members, Add/Delete Untagged Members, or Move Port to Current VLAN.
2. Click on a port to change its state:
   - ❑ For Add/Delete Port Members, clicking on a a darkened port adds it to the VLAN, while clicking on a VLAN member deletes it. The status of the port on any other VLAN remains unchanged.
   - ❑ For Add/Delete Untagged Members, clicking on a darkened port adds it to the untagged set, and clicking on a green dot changes it to an untagged port. Clicking on an untagged port changes it to a tagged port. The status of the port on any other VLAN remains unchanged.
   - ❑ Move Port to Current VLAN is the same as Add/Delete Port Members, except it also removes the port from any other VLAN of which it is a member.

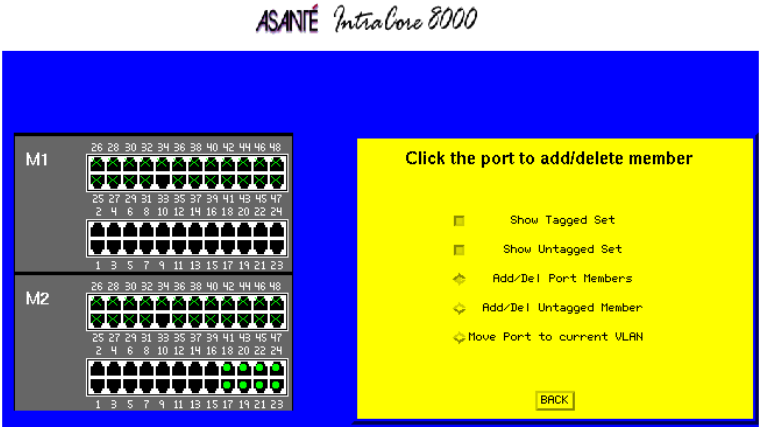


Figure 5-16 Add/Delete Port Member dialog box

To add or delete MAC addresses for devices connected to the IntraCore 8000, click the **Add/Del MAC Addr** button in the VLAN Group Configuration dialog box. The dialog box shown in Figure 5-17 appears.

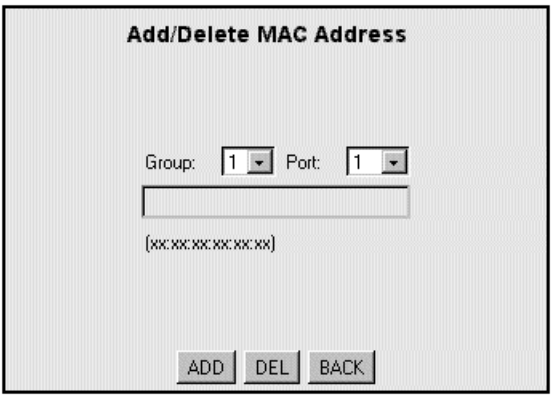


Figure 5-17 Add/Delete MAC Address dialog box

When you have added or deleted the MAC address, the VLAN Group Configuration page is displayed again.

Duplicate IP Button

This button lights up if a duplicate IP number has been detected on the system. If you click the button, it opens the Duplicate IP Trap Log page which, if the trap is enabled, displays a record of duplicate IP Addresses detected. The Log shows the MAC address of the device that is the original or rightful owner of the IP address, and the MAC address of the spoofer device that is using a copy of the IP address.

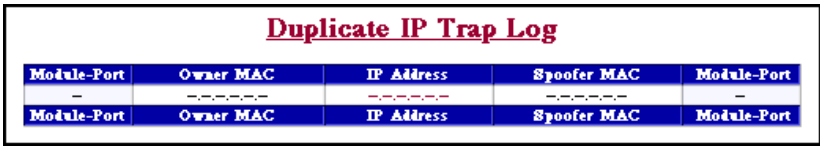


Figure 5-18 Duplicate IP Trap Log page

For more information on enabling the Duplicate IP trap, see “Enabling and Disabling Duplicated IP Trap” on page 4-11.

A
Technical Support

Contacting Technical Support

To contact Asanté Technical Support:

Telephone	(800) 622-7464
Fax	(801) 566-3787
Fax-Back	(800) 741-8607
E-mail	support@asante.com
World Wide Web Site	http://www.asante.com
FTP site for RMON information	<ftp://ftp.isi.edu/in-notes/rfc1757.txt>

Technical Support Hours

6:00 a.m. to 5:00 p.m. Pacific Standard Time USA, Monday - Friday.

B
MIB Statistics

MIB Object Definitions for Counters

The following MIB objects are those for which counters are displayed in the Statistics Counters screens shown in both the console and Web interface. The definitions and references are quoted from RFC 1516.

Readable Frames

"This object is the number of frames of valid frame length that have been received on this port. This counter is incremented by one for each frame received on this port whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize (Ref: IEEE 802.3 Std, 4.4.2.1) and for which the FCSError and CollisionEvent signals are not asserted.

This statistic provides one of the parameters necessary for obtaining the packet error rate. The approximate minimum time for rollover of this counter is 80 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aReadableFrames

Readable Octets

"This object is the number of octets contained in valid frames that have been received on this port. This counter is incremented by OctetCount for each frame received on this port which has been determined to be a readable frame (i.e., including FCS octets but excluding framing bits and dribble bits).

This statistic provides an indicator of the total data transferred. The approximate minimum time for rollover of this counter is 58 minutes."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aReadableOctets

FCS Errors

"This counter is incremented by one for each frame received on this port with the FCSError signal asserted and the FramingError and CollisionEvent signals deasserted and whose OctetCount is greater than or equal to

minFrameSize and less than or equal to maxFrameSize (Ref: 4.4.2.1, IEEE 802.3 Std).

The approximate minimum time for rollover of this counter is 80 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aFrameCheckSequenceErrors

Alignment Errors

"This counter is incremented by one for each frame received on this port with the FCSError and FramingError signals asserted and CollisionEvent signal deasserted and whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize (Ref: IEEE 802.3 Std, 4.4.2.1). If rptrMonitorPortAlignmentErrors is incremented then the rptrMonitorPortFCSErrors Counter shall not be incremented for the same frame.

The approximate minimum time for rollover of this counter is 80 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aAlignmentErrors

Frame Too Longs

"This counter is incremented by one for each frame received on this port whose OctetCount is greater than maxFrameSize (Ref: 4.4.2.1, IEEE 802.3 Std). If rptrMonitorPortFrameTooLongs is incremented then neither the rptrMonitorPortAlignmentErrors nor the rptrMonitorPortFCSErrors counter shall be incremented for the frame.

The approximate minimum time for rollover of this counter is 61 days."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aFramesTooLong

Short Events

"This counter is incremented by one for each CarrierEvent on this port with ActivityDuration less than ShortEventMaxTime. ShortEventMaxTime is greater than 74 bit times and less than 82 bit times. ShortEventMaxTime has tolerances included to provide for circuit losses between a conformance test point at the AUI and the measurement point within the state machine.

Note: shortEvents may indicate externally generated noise hits which will cause the repeater to transmit Runts to its other ports, or propagate a collision (which may be late) back to the transmitting DTE and damaged frames to the rest of the network.

Implementors may wish to consider selecting the ShortEventMaxTime towards the lower end of the allowed tolerance range to accommodate bit losses suffered through physical channel devices not budgeted for within this standard.

The approximate minimum time for rollover of this counter is 16 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aShortEvents

Runts

"This counter is incremented by one for each CarrierEvent on this port that meets one of the following two conditions. Only one test need be made.

a) The ActivityDuration is greater than ShortEventMaxTime and less than ValidPacketMinTime and the CollisionEvent signal is deasserted.

b) The OctetCount is less than 64, the ActivityDuration is greater than ShortEventMaxTime and the CollisionEvent signal is deasserted. ValidPacketMinTime is greater than or equal to 552 bit times and less than 565 bit times.

An event whose length is greater than 74 bit times but less than 82 bit times shall increment either the shortEvents counter or the runts counter but not both. A CarrierEvent greater than or equal to 552 bit times but less than 565 bit times may or may not be counted as a runt.

ValidPacketMinTime has tolerances included to provide for circuit losses between a conformance test point at the AUI and the measurement point within the state machine.

Runts usually indicate collision fragments, a normal network event. In certain situations associated with large diameter networks a percentage of collision fragments may exceed ValidPacketMinTime.

The approximate minimum time for rollover of this counter is 16 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aRunts

Collisions

"This counter is incremented by one for any CarrierEvent signal on any port for which the CollisionEvent signal on this port is also asserted.

The approximate minimum time for rollover of this counter is 16 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aCollisions

Late Events

"This counter is incremented by one for each CarrierEvent on this port in which the CollIn(X) variable transitions to the value SQE (Ref: 9.6.6.2, IEEE 802.3 Std) while the ActivityDuration is greater than the LateEventThreshold. Such a CarrierEvent is counted twice, as both a collision and as a lateEvent.

The LateEventThreshold is greater than 480 bit times and less than 565 bit times. LateEventThreshold has tolerances included to permit an implementation to build a single threshold to serve as both the LateEventThreshold and ValidPacketMinTime threshold.

The approximate minimum time for rollover of this counter is 81 hours."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aLateEvents

Very Long Events

"This counter is incremented by one for each CarrierEvent on this port whose ActivityDuration is greater than the MAU Jabber Lockup Protection timer TW3 (Ref: 9.6.1 & 9.6.5, IEEE 802.3 Std).

Other counters may be incremented as appropriate." Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aVeryLongEvents

D.R. Mismatches

"This counter is incremented by one for each frame received on this port that meets all of the following conditions:

a) The CollisionEvent signal is not asserted.

b) The ActivityDuration is greater than ValidPacketMinTime.

c) The frequency (data rate) is detectably mismatched from the local transmit frequency.

The exact degree of mismatch is vendor specific and is to be defined by the vendor for conformance testing.

When this event occurs, other counters whose increment conditions were satisfied may or may not also be incremented, at the implementor's discretion. Whether or not the repeater was able to maintain data integrity is beyond the scope of this standard."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aDataRateMismatches

Auto Partitions

"This counter is incremented by one for each time the repeater has automatically partitioned this port. The conditions that cause port partitioning are specified in the partition state machine in Section 9 [IEEE 802.3 Std]. They are not differentiated here."

Reference: IEEE 802.3 Rptr Mgt, 19.2.6.2, aAutoPartitions

Total Errors

"The total number of errors which have occurred on this port. This counter is the summation of the values of other error counters (for the same port), namely:

rptrMonitorPortFCSErrors,

rptrMonitorPortAlignmentErrors,

rptrMonitorPortFrameTooLongs,

rptrMonitorPortShortEvents,

rptrMonitorPortLateEvents,
rptrMonitorPortVeryLongEvents, and

rptrMonitorPortDataRateMismatches.

This counter is redundant in the sense that it is the summation of information already available through other objects. However, it is included specifically because the regular retrieval of this object as a means of tracking the health of a port provides a considerable optimization of network management traffic over the otherwise necessary retrieval of the summed counters."